TABLE OF CONTENTS

SUMMARY 3
Catalyst 3
Ovum view 4
Key messages 4

THE INSIDER THREAT IS REAL; MORE EFFORT IS NEEDED BY ALL ORGANIZATIONS AND NATIONS TO DEAL WITH IT 4

Japanese and ASEAN organizations have and continue to be breached by insider attacks 4
Japan and ASEAN spending on security software continues to rise but remains lower than the global average 6
Globally the most dangerous insiders have privileged access but not all countries recognize this 7
Concern about insider threats continues 8
The majority of enterprise data is still held on databases and servers, but cloud is catching up fast 9

NEAR NEIGHBORS PROVIDE DIFFERENT INSIDER THREAT AND DATA PROTECTION INSIGHTS 11

Japan focuses on the threats posed by ordinary employees 11

CLOUD AND BIG DATA PROJECTS ARE SHOWN TO SUFFER FROM SERIOUS DATA PROTECTION ISSUES 11

Large volumes of customer-sensitive data need to be protected 11

MANAGEMENT SUMMARY AND RECOMMENDATIONS FOR ENTERPRISES 14

OUR SPONSORS
SUMMARY

Catalyst

The number and range of insider attacks on business systems, and the data losses that continue to be reported, show no signs of relenting. The negative impact on the organizations involved, and on their clients, customers, and business associates, often makes recovery difficult and the associated trust issues long-lasting.

The Japan and ASEAN edition of the 2015 Insider Threat Report provides present-day insight and opinion into the host of data breach threats that enterprise organizations across the region face on a daily basis. The report is based on an online survey conducted on Vormetric's behalf by Harris Poll in Fall 2014, with survey responses from 818 senior business managers and IT professionals in major global markets. Of these respondents 102 were from Japan and 103 from the ASEAN region, principally Indonesia, Malaysia, the Philippines, Singapore, and Thailand. Their views are insightful, as are their opinions on the types of user that put key business information assets at most risk. This version of the Insider Threat Report provides the opportunity to analyze the security and risk responses from Japanese and ASEAN regional experts and compare their feedback to that of their counterparts in the U.S. and Europe.

It may seem like a contradiction in terms but, insider threats are caused by an ever-widening range of offenders, and as the threat landscape grows it becomes more difficult to deal with. Threats come from individuals or groups who maliciously or accidentally do things that put an organization and its data at risk. The range of miscreants has moved beyond everyday employees and IT staff. It now includes malicious outsiders with the skills needed to steal valid user credentials, and business partners, suppliers, contractors, and third-party service providers with excessive access rights. Unless they are securely controlled and managed, all of these individuals have the opportunity, and in many cases the technical skills, to get inside corporate networks and steal corporate information assets.
Ovum view

The 2015 Insider Threat Report shows that insider threat awareness levels have increased. Globally, only 11% of respondents felt that their organization was not vulnerable to insider attacks. At the same time, a very large percentage (93%) were looking to increase or maintain existing spending on IT security and data protection in the coming year.

There are, however, substantial regional differences. 85% of Japanese and ASEAN respondents felt that their organization was now more at risk from an insider attack, leaving 15% of survey respondents claiming they are not vulnerable.

90% of Japanese and ASEAN respondents say their organizations were looking to increase or at least maintain their security spend during the year ahead. However, after examining the detailed information available, the ASEAN position looks to be significantly more proactive. The vast majority of ASEAN survey respondents are looking to increase their security spend. However, over in Japan, organizations have established more of a holding position, with most planning to maintain security spend at 2014 levels.

Key messages:

• 85% of Japanese and ASEAN respondents felt that their organization was now more at risk from an insider attack.

• Japanese respondents believe that ordinary users (56%) pose the biggest internal threat to corporate data; privileged users are well down the list at 37%.

• ASEAN aligns itself and then exceeds the global position (62%) when putting privileged users at the top of the at-risk list.

THE INSIDER THREAT IS REAL; MORE EFFORT IS NEEDED BY ALL ORGANIZATIONS AND NATIONS TO DEAL WITH IT

Japanese and ASEAN organizations have and continue to be breached by insider attacks

The increasing number of data breaches reported over the last 12 months and the resultant data losses have hit business organizations hard. All major markets and industry verticals have been affected. The financial and reputational effect can continue to have a significant, detrimental impact on the businesses concerned for a long period of time after the event.

Data breaches are happening everywhere, and the Japanese and ASEAN markets are not immune. However, for Japan and ASEAN, it is generally the case that only the more serious data breaches make it into the public domain and, even then, the amount of information made available for public consumption is usually limited.
Across the Japan and ASEAN region, regulatory authorities respond to data breaches and take appropriate actions that are often not reported at the time, and only become public after the event and when sanctions have been exacted.

These are relevant issues because 48% of ASEAN organizations and 29% of Japanese respondents say their organizations have encountered a data breach or failed a compliance audit in the last year. The ASEAN numbers are well above the global average and worse than those reported in any other region. Japan was at the lower end of the scale, with only Germany reporting lower data breach numbers. The impact of the respective positions comes across very clearly when comparing the reasons organizations have for protecting data. The number of ASEAN respondents who cited a data breach they had already experienced was double that of their Japanese neighbors.

While accepting that these are only the tip of a very large iceberg, recent insider attacks and data breaches that have affected companies in the Japan and ASEAN region include the following:

- Singapore-based telecoms service provider M1 had to shut down its pre-order, web page facility for the new Apple iPhone for a period of time, after a cookie modifier plug-in was found to have been used by a technically skilled insider to access personal customer data.

- A phishing attack resulted in the theft of personal information belonging to customers of Japan Airlines’ frequent flier club. Available information suggests that between 110,000 and 750,000 members of the program could have been affected and that the breach remained active and undetected for over a month.

- Third-party service provider fraud resulted in the Monetary Authority of Singapore (MAS) taking action against Standard Chartered Bank when data from over 600 private banking clients was stolen.

- The 2013 Yahoo Japan Data Breach resulted in the login names of 22 million accounts being put at risk when 10% of the user credentials the company held were exposed by attackers.

- The K Box Entertainment Group, of Singapore is alleged to have suffered a serious data security breach when the personal data of over 300,000 customers was leaked during hacktivist activities.

- Third-party contractor fraud in South Korea at KB Kookmin Card, Lotte Card and NH NongHyup Card, where a portable hard drive device was used to copy the details of around 20 million credit card customers.
64% of ASEAN respondents say that their organizations have security spending increases planned.

Only 26% of Japanese respondents say that their organizations plan security spending increases, 62% are maintaining security spending levels.

Threat activities are ongoing. The Japanese National Institute of Information and Communications Technology (NICT), which has a network of 250,000 sensors, said that last year there were 25.66 billion attempts to compromise systems. When the survey was first carried out in 2005 it recorded just 310 million attempts to breach security.

Reported breaches have resulted in regulatory scrutiny and action taken against organizations that had not done enough to fulfill regulatory compliance standards. Across the region and in particular in Singapore, Malaysia, and the Philippines, countries have introduced new and more comprehensive data protection regimes.

For organizations that now have to meet these new and evermore challenging data protection requirements, the deployment of technology solutions that provide improved levels of access control, user monitoring, and data protection provide a way forward to ensure that networks and systems remain secure and address existing vulnerabilities.

As a direct result of the growing number of data breaches that are belatedly making their way into the public domain from across the region, Japanese and ASEAN organizations are becoming more accepting of their data protection responsibilities. This is highlighted by the percentage of senior business and IT managers who said that their organizations are looking to increase spending on security in the next 12 months.

**Japan and ASEAN spending on security software continues to rise, but remains lower than the global average**

The global version of the Insider Threat Report identified that only 7% of respondents say their organizations felt that they were in a position to spend less on data protection in the year ahead. The Japan and ASEAN position is similar but there are regional differences and also variations within the region itself.

![Threat Levels (Percent)](image)

Figure 1: Increased security spending across the Japan and ASEAN region including comparisons to other major markets
Globally, 56% of survey respondents were looking to increase their security spending to deal with insider threats in the coming year, and the remaining 37% were looking to consolidate and spend the same amount as last year. The survey results in Figure 1 show that ASEAN spending levels on security match the global average and that 93% expect to increase or maintain their security budgets. What it doesn’t identify is that 64% of ASEAN respondents say their organizations have substantial security increases planned and only 29% are looking to maintain a holding position.

That said, the Japanese position is somewhat different. The headlines show that 88% plan to increase or maintain security spending. However, of that 88%, almost three quarters were only looking to maintain existing spending levels and only 26% were taking a positive stance.

Overall, Ovum research shows that annual spending increases on security products exceeded the 10% mark last year, and our projections suggest that 2015 will see similar global levels of double-digit growth. However, the lack of focus is worrying. We believe that more attention is needed on areas of data protection and security facilities that control access to business systems and the company-sensitive information they hold.

Globally the most dangerous insiders have privileged access, but not all countries recognize this

As shown in Figure 2, Japanese organizations believe that the greatest threat to their data assets comes from everyday business users, whereas the rest of the ASEAN region places privileged users as the highest risk group. The ASEAN position matches up with the global statistics, but at 62% its percentage figures on privileged user risk exceeds all other markets including the levels of concern expressed by U.S. enterprise organizations.

Historically, systems administrators and other business users with elevated access privileges have not had the right levels of control imposed on their activities. Their often unchallenged ability to gain access to, and make copies of, company-sensitive data has put business systems at risk.

Today, only half of all business organizations have deployed privileged access/identity management (PAM or PIM) technology.* But this only represents the global average figure and within it there are country-level inconsistencies. For example, within the Japan and ASEAN region, Japanese organizations do not accept that privileged users pose much of a threat when their activities are compared to everyday business users.

“GLOBALLY AND IN ASEAN PRIVILEGED USERS ARE RECOGNIZED AS THE MOST DANGEROUS INSIDERS (62%).”

*Source: Ovum ICT Enterprise Insights—Major Markets Technology Priorities, October 2013—a global study with 6,700 respondents
In most mature global markets, senior management concerns over privileged user access have now reached the top of the security agenda. They understand the damage that unrestricted access to corporate data assets can cause. They also recognize that if this type of user is not properly monitored and controlled, the harm caused to the business can be far-reaching.

At 55% the global position for privileged users puts it at the top of the risk list. Unsurprisingly given the notoriety of Edward Snowden and the uproar following the Target and Home Depot breaches, third-party contractors and service providers were in second place. In third place and not far behind were business partners who have access to company networks.

These are the global positions and, as shown in Figure 3, most of these are mirrored by the ASEAN position. Regional differences come into play when the Japanese figures are examined and concerns about the security position of ordinary employees and contractors and service providers exceeds that of other major markets.

**Concern about insider threats continues**

The number of successful insider attacks continues to rise. Throughout the APAC region, which includes Japan and ASEAN, regulations are being strengthened and data protection requirements bolstered.

Ovum research shows that average breach detection timescales are still measured in months and remain far too high. It was therefore no surprise to find that the vast majority of Japan and ASEAN respondents to the Vormetric threat survey (85%) felt their organizations were vulnerable to an insider attack. This figure, although lower than the 89% average from the global survey, continues to show that protection of corporate data resources needs to be improved and that business concerns about shortfalls in data protection are valid and continue to be expressed.

In Japan privileged users take third place (37%), behind ordinary employees (56%) and contractor/service provider employees (52%).

Respondents from enterprises around the globe express high levels of anxiety—83% to 91% of respondents feel their organizations are vulnerable. Japan (86%) and ASEAN (84%) are typical of other global results.
Figure 4 shows there are small regional differences between Japan and ASEAN, the U.S., and other major markets, but whether the reported concerns are set at 86/84% for Japan and ASEAN or 93% as is the case for the U.S., the consistent theme remains of high-level enterprise anxiety. Taking the global average, only 11% felt that their organizations were safe from insider threats. At an average figure of 15% across the Japanese and the ASEAN regions, the numbers confirm that despite increases in security spending, most organizations continue to be worried about insider activity and recognize they are not in complete control of the situation.

The majority of enterprise data is still held on databases and servers, but cloud is catching up fast

Globally the top three locations by volume where company-sensitive data is stored and must be protected are: databases (47%), file servers (39%), and cloud (37%). The position may be fairly consistent across most major geographies, but there are recognizable regional differences.

Cloud and more recently the associated adoption of cloud-based Big Data services are driving increased data protection concerns. Across all markets, and in particular within the ASEAN region, levels of anxiety are growing in line with the increased data volumes and the amount of company-sensitive data that now needs to be protected.

Worries about a lack of control over third-party access; the use of third-party systems administrators; and data locational issues when foreign intervention and legal sovereignty come into play all make the case for improving cloud and Big Data protection.

Another discussion that needs to take place revolves around the perception of risk that mobile devices and user mobility have brought to the table. By comparison to other major data storage areas (databases, servers, and cloud), only 20% of sensitive company data is held on mobile devices and, of that 20%, a large proportion is being held on company-owned devices.

In our opinion the discussion shouldn’t really be about the data volumes involved. The real concern for the business managers is firmly about the lack of control over the mobile devices that are in use. It is also about not having enough information to know what data has been copied to those devices and not having the controls in place to stop copies of company-sensitive data being made.

Good quality monitoring and access control technology provide part of the answer. But irrespective of where the data is being held, it is important to know and be able to control who gets access and what they can do with that access. This provides the ability to highlight and report on misuse that could otherwise put company-sensitive data at risk.

In Japan mobile risk...is seen as representing a risk position far greater than actual usage volumes.
Figures 6 and 7 highlight the differences between Japan and ASEAN and the global position on risk. They also highlight the inter-regional differences between Japan and ASEAN.

For Japan, the higher than average levels of data that remain on premise within database and file server repositories and the lower than average cloud and Big Data usage provides a risk position that fits with the volumes involved. However, by comparison to other markets, it understates the cloud security risk position. By far, the areas that are most out of line are mobile, which is seen as representing a risk position far greater than actual usage volumes and end user PCs and workstations which provide a similar usage-to-risk profile. Both these positions and the devices involved go some way to explaining the Japanese obsession with ordinary business users as the highest “at-risk” user group.

Similarly to the Japanese position, the higher than average use of on-premise databases and file servers is reflected in the usage versus risk position taken by organizations in the ASEAN region.

This is the only region where file server usage challenges for the number one data storage position alongside databases. It is also the only region where Big Data usage is reported to be higher than general cloud adoption. By comparison to its near neighbor Japan, business use of mobile is low and the associated risk profile is less than a third of that reported by Japanese respondents (19% versus 58% for Japan).
NEAR NEIGHBORS PROVIDE DIFFERENT INSIDER THREAT AND DATA PROTECTION INSIGHTS

Japan focuses on the threats posed by ordinary employees

Japan sees insider threats differently from every other major market. As highlighted earlier in the report and as shown in Figure 8, Japanese respondents continue to see everyday business users as providing the highest levels of threat to corporate information systems. This is also a position that differentiates Japanese organizations from those in ASEAN. All ASEAN countries position privileged users as providing the greatest threat to sensitive company data, whereas at 38% the Japanese number is a significant 18 percentage points below the global average and 24 percentage points below the ASEAN position.

The global report identifies privileged users as the group that poses the highest levels of risk to enterprise organizations. Japan focuses on ordinary employees (57%), contractors and services providers (53%), while privileged users (38%) are seen as lower risk.

CLOUD AND BIG DATA PROJECTS ARE SHOWN TO SUFFER FROM SERIOUS DATA PROTECTION ISSUES

Large volumes of customer sensitive data need to be protected

Within all markets the cloud and Big Data issues revolve around the need to protect more data assets, the distributed nature of those assets, and the growing number of users, often employed by third-party service providers who are going to need access. With four out of five enterprise organizations already making use of cloud-based services, the amount of company sensitive data that needs to be protected is growing fast. Cloud and Big Data usage would undoubtedly be more extensive already if the major security challenges had been overcome at an earlier stage.

“Japanese enterprise show a low deployment rate of sensitive data to cloud environments (44%) when compared against ASEAN (56%) and the U.S. (60%).”
80% of respondents’ organizations make use of some form of cloud-based services, and often this involves multiple cloud deployments. The 20% who say they choose not to participate have expressed specific security and operational reasons why not.

Nevertheless, the usage figures drop away sharply to just over 50% when mission-critical applications are being considered. But even then, the 50% average varies across the major markets.

The cloud adoption figures for ASEAN when holding sensitive data in the cloud are comparatively on the high side at 56%, but there is a further difference when the ASEAN position is compared to its near neighbor Japan. As shown in Figure 8, the Japanese adoption rate falls away to 44% when sensitive company data is involved, leaving it below the major European market of Germany and level with the UK. It is also significantly below the U.S. which at 60% accepts a higher level of cloud risk than any other market.

![Figure 9: The percentage of organizations holding company sensitive data in the Cloud](image)

“ASEAN SHOWS HIGH ADOPTION LEVELS FOR BIG DATA IMPLEMENTATIONS WITH SENSITIVE DATA AT 41% WITH JAPAN REPRESENTING THE OPPOSITE END OF THE SPECTRUM AT 12%.”

Big Data adoption also shows significant differentiation between Japan and ASEAN. Within the region ASEAN organizations reported the highest levels of adoption and concern when protecting sensitive data in Big Data environments.

This issue positions the high usage Big Data markets of ASEAN and the U.S. alongside each other, with lower Japanese adoption and usage effectively lowering the perception of risk felt by that particular market.
Even though Big Data projects generally rely on the cloud-based service delivery model to support high processing and data throughput overheads, overall lower usage levels in markets such as Japan continue to soften the all-round perception of risk. Figure 10 shows that the adoption of big data projects within all regions has a direct correlation between adoption and risk, with the risk element consistently sitting slightly below usage and therefore sitting below actual data risk levels.

Adoption of Big Data projects across ASEAN outstrips that of Japan, which once again is reflected in the regional appreciation of risk. This is highlighted in Figure 11, with security and data protection risk responses that are consistently higher across the ASEAN region compared to the same risk responses from Japanese organizations.
MANAGEMENT SUMMARY AND RECOMMENDATIONS FOR ENTERPRISE

In news reporting across all geographies and industry verticals, the number of organizations that have suffered a security breach and had company sensitive data stolen has risen sharply. Insider threats, caused by employees, business partners, suppliers, contractors, third-party service providers, and outsiders using stolen credentials, have made a substantial contribution to the data loss numbers reported and must be addressed to improve the situation.

This report focuses on the main insider threat issues that are causing concern to senior business and IT managers within the Japanese and ASEAN regions. As was found to be the case further afield in the U.S. and Europe, the majority of Japanese and ASEAN company-sensitive data continues to be stored on-premise on corporate databases and servers. At the same time Japan and ASEAN has seen significant cloud and Big Data adoption, but not at even levels of consistency. The percentage of ASEAN organizations prepared to hold company sensitive data in the cloud is 56%, a figure that is only exceeded by the U.S., whereas Japanese response levels were more conservative and down in the mid-forties, aligning Japan with the results from Germany and the UK. For Big Data projects there were differences too. ASEAN organizations expressing data protection concerns about Big Data projects were three times higher than their Japanese neighbors, a factor that was reasonable because adoption levels were also three times greater in the ASEAN region than in Japan.

However, irrespective of the respective levels of cloud and Big Data adoption, the volumes continue to grow and because of this better and more integrated data protection strategies are required. These should involve the use of cryptographic, encryption-based data protection and key management and the use of strong authentication and access controls. Data monitoring and technologies such as security information and event management (SIEM) to identify unusual or malicious data usage patterns are also necessary.

Maintaining the right levels of access for authorized users is an important issue that organizations continue to struggle with. Too much access puts corporate systems and their data at risk, reducing it below acceptable levels affects operational efficiency and can become an unacceptable burden for everyday business users.

What organizations should be looking for to keep their data safe is a unified protection strategy that involves the use of layered security that fits in with their risk profile. When asked about which insiders caused the greatest levels of concern ASEAN organizations focused on privileged account users, whereas Japanese companies were more worried about ordinary employees. They were both right, but equally all other groups of insiders including executive managers, and other IT staff who often seem to operate below the security radar should be given greater consideration. They, along with all other groups of insiders, have the potential and often the skills to put company sensitive data at risk.
ANALYST PROFILE—ANDREW KELLETT, PRINCIPAL ANALYST SOFTWARE—IT SOLUTIONS, OVUM

Andrew enjoys the challenge of working with state-of-the-art technology. As lead analyst in the Ovum IT security team, he has the opportunity to evaluate, provide opinion, and drive the Ovum security agenda, including its focus on the latest security trends. He is responsible for research on the key technologies used to protect public and private sector organizations, their operational systems, and their users. The role provides a balanced opportunity to promote the need for good business protection and, at the same time, to research the latest threat approaches.

HARRIS POLL—SOURCE/METHODOLOGY

Vormetric’s 2015 Insider Threat Report was conducted online by Harris Poll on behalf of Vormetric from September 22-October 16, 2014, among 818 adults ages 18 and older, who work full-time as an IT professional in a company and have at least a major influence in decision making for IT. In the U.S., 408 ITDMs were surveyed among companies with at least $200 million in revenue with 102 from the health care industries, 102 from financial industries, 102 from retail industries and 102 from other industries. Roughly 100 ITDMs were interviewed in the UK (103), Germany (102), Japan (102), and ASEAN (103) from companies that have at least $100 million in revenue. ASEAN countries were defined as Singapore, Malaysia, Indonesia, Thailand, and the Philippines. This online survey is not based on a probability sample and therefore no estimate of theoretical sampling error can be calculated.

ABOUT VORMETRIC

Vormetric (@Vormetric) is the industry leader in data security solutions that protect data-at-rest across physical, Big Data and cloud environments. Vormetric helps over 1500 customers, including 17 of the Fortune 30, to meet compliance requirements and protect what matters—their sensitive data—from both internal and external threats. The company’s scalable Vormetric Data Security Platform protects any file, any database and any application’s data—anywhere it resides—with a high performance, market-leading solution set.

FURTHER READING
