Sharing the blame
How companies are collaborating on data security breaches
A report from The Economist Intelligence Unit
Contents

Introduction 2
About the research 4
The situation in Asia 6
The current response 9
What the future holds 14
Conclusion 17
Introduction

As the type, quantity and complexity of data collected by companies increases, organisations face significant challenges in securely gathering and storing information. The free movement of data across borders, through public and corporate networks, has made it particularly difficult to safeguard this information and protect it against security breaches.

Fragmented legislative environments across Asia make data protection harder, with governments finding it difficult to create harmonious regulations covering data usage or provide consistent guidance on how to deal with security breaches. While regulation will take some time to catch up, companies can partly address this by taking the lead in disclosing data security breaches.

This research project set out to explore the ways in which organisations are collaborating to deal with the disclosure of data security breaches. How are they co-operating with governments, other companies and third parties in areas such as requirements for the public disclosure of such breaches? Do they have consistent cyber security policies? To what extent are they sharing best practices?

The research, based primarily on a survey of over 200 senior executives across Asia and interviews with a number of corporate executives and data-security experts, finds that the occurrence of data breaches is alarmingly high, with only 35% of firms confident that they haven’t experienced a breach in the last 12 months. Despite this apparent failure to protect data, firms are not blaming their IT systems. Rather, the high level of reported trust in their organisation’s IT (expressed by 85% of respondents) illustrates acceptance of the reality that data breaches are going to occur regardless of the quality of companies’ IT systems. The Heartbleed bug, a newly discovered security vulnerability that puts users’ passwords at many popular websites at risk, is a recent example of all IT systems being vulnerable to attack. With this in mind, companies are looking at ways of proactively taking the lead in limiting the damage when breaches do take place.

How companies will effectively deal with breaches in the future is unclear. What is clear is that they must do so: almost 40% of firms in Asia report significant economic loss as a result of data-security issues. Driven by this, companies are increasingly looking to collaborate to minimise the impact of such breaches, particularly when they see the positive reputational benefit that disclosure and collaboration can bring.
Four things businesses should know about data breaches in Asia

**Occurrence of data breaches is alarmingly high:**
Only 35% of firms are confident that they haven’t experienced a data breach in the last 12 months.

**Businesses regard data security as extremely important:**
76% say it is high priority and only 8% regard it as low priority.

**Data security breaches are hurting companies financially:**
Almost 40% of firms have experienced significant economic loss as a result of data security breaches.

**Companies are better placed than government to deal with data security breaches:**
Over 80% of respondents say that the best way to minimise data security breaches is for business to proactively take the lead.
Sharing the blame: How companies are collaborating on data security breaches is an Economist Intelligence Unit (EIU) report, commissioned by Akamai. The EIU conducted a survey from October to December 2013 of 210 senior executives from across the Asia-pacific region. Respondents came from a range of industries including 32% from financial and professional services firms, 47% of which held c-level positions across a range of functions from general management to operations.

In addition, the EIU conducted in-depth interviews with a range of senior executives and analysts. Given the sensitivity of the issue some interviewees have been anonymised. The report was written by Robert Clark and edited by Charles Ross.

Totals may not add up to 100% either due to rounding or because respondents could select more than one answer.
We would like to thank all those who participated in the survey and the interviews for their time and insight. The EIU bears sole responsibility for the content of this report.
With close to 50% of the world’s internet users, Asia is buzzing with online transactions from mobile devices, computers and other internet-enabled devices. Financial and personal information is being submitted and stored online at a frantic pace as consumers and businesses alike embrace the advantages of managing their daily transactions online. The financial and personal transactions undertaken generate valuable data that needs protecting.

The survey conducted for this report shows that in Asia this data remains far from secure. Some 38% of companies have experienced a data breach in the past year, with a further 26% unaware of whether a breach has occurred at all. In the past five years, 53% of companies have experienced a breach. Alarmingly, 5% of all companies have experienced 50 or more. (Figure 1).

With less than one-fifth of companies sure that the data they hold has not been compromised in the past five years, companies might be expected to be sceptical about the security of their systems. Yet confidence in IT security systems remains high, with 85% of executives rating their systems as very or quite trustworthy (Figure 2). The

---

**Figure 1: Disturbingly common**

<table>
<thead>
<tr>
<th>Number of data security breaches our firm has experienced (%) respondents</th>
<th>In the last 12 months</th>
<th>In the last 5 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 breaches</td>
<td>35%</td>
<td>18%</td>
</tr>
<tr>
<td>1 to 5 breaches</td>
<td>32%</td>
<td>29%</td>
</tr>
<tr>
<td>6 to 10 breaches</td>
<td>2%</td>
<td>11%</td>
</tr>
<tr>
<td>11 to 50 breaches</td>
<td>3%</td>
<td>8%</td>
</tr>
<tr>
<td>&gt;50 breaches</td>
<td>1%</td>
<td>5%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>26%</td>
<td>28%</td>
</tr>
</tbody>
</table>

Source: The Economist Intelligence Unit.
confidence level rises to 92% at financial services companies, even though just 14% are certain they have had no breaches in the past five years.

Even more perplexing in light of the high level of trust companies place in their IT systems is the amount of economic loss firms experience as a result of breaches. Nearly 40% of respondents say data security breaches have caused a significant economic loss to their firm (Figure 3). Financial services firms are the worst hit, with half reporting a significant loss.

Larger companies also say they have been affected more than smaller firms, with 56% of large firms (those with between US$5bn and US$10bn in global annual revenues), and 51% of very large firms (with revenues above US$10bn), reporting losses as a result of data security issues.

With data breaches a common occurrence and the losses resulting from these significant, data security remains a high priority for companies across Asia. Three-quarters of respondents (76%) place a high priority on data security with only 8% regarding it as low priority.

**Figure 2: Trust in your IT system**

Level of trust we have in our IT system keeping data secure (% respondents)

<table>
<thead>
<tr>
<th>Level of trust</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very trustworthy, my organisation’s IT system is extremely secure</td>
<td>19%</td>
</tr>
<tr>
<td>Quite trustworthy, my organisation’s IT system does a pretty good job at safeguarding data most of the time</td>
<td>66%</td>
</tr>
<tr>
<td>Not trustworthy, my organisation’s IT system is vulnerable to data security breaches</td>
<td>12%</td>
</tr>
<tr>
<td>I don’t know</td>
<td>3%</td>
</tr>
</tbody>
</table>

Source: The Economist Intelligence Unit.

**Figure 3: Taking a hit**

Data security breaches cost our firm a significant amount of money (% respondents)

<table>
<thead>
<tr>
<th>Agreement</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>39%</td>
</tr>
<tr>
<td>Neither agree nor disagree</td>
<td>31%</td>
</tr>
<tr>
<td>Disagree</td>
<td>21%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>10%</td>
</tr>
</tbody>
</table>

Source: The Economist Intelligence Unit.

**Figure 4: Big firms, bigger worries**

Priority our organisation places on data security (% respondents)

<table>
<thead>
<tr>
<th>Priority level</th>
<th>$500m or less</th>
<th>$500m to $1bn</th>
<th>$1bn to $5bn</th>
<th>$5bn to $10bn</th>
<th>$10bn or more</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highest priority, has full attention of senior management &amp; board</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High priority, recognised as important</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate priority, only limited attention from senior management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low priority, considered just one of many IT problems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not important at all</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: The Economist Intelligence Unit.
Smaller businesses (with annual revenues below US$500m) put less emphasis on data security—69% rank it as high or highest priority, compared to 83% of large companies and 89% of very large businesses (Figure 4). Because of their size, smaller companies suffer fewer breaches than their large counterparts. But it is telling that 36% of small companies have suffered one to five breaches in the last year, more than all the larger business segments.

Among industry sectors, IT companies take data security the most seriously, with 85% rating it high priority, followed by manufacturing (84%), professional services (79%) and financial services (78%).

Security policies are inherently difficult to implement and manage because of the varied ways in which breaches can occur. Ranging from staff carelessness to malicious attacks, the most likely data breach is through the loss or theft of a device such as a laptop, smartphone or tablet. Nearly half (47%) of all companies have experienced data loss through a missing device in the past five years. Just over a quarter (26%) say they have lost data through an accidental leak online (Figure 5).

For all companies, intrusion and theft rank as the third most likely breach (cited by 21%), but at smaller companies and large companies it ranks second. It is also the second highest cause of data loss for manufacturers (27%).

Financial services businesses face some of the most targeted malicious attacks. One worrying trend, says the head of security at a very large Asia-Pacific financial services company (with revenues greater than US$10bn), is that “corporate espionage is also a reality, with competitors striving to obtain internal information by gaining access to company calendars and customer data.”

Corporate espionage is also a reality, with competitors striving to obtain internal information by gaining access to company calendars and customer data.

Security Chief, Asia-Pacific financial services firm

Figure 5: Attacked from all sides

<table>
<thead>
<tr>
<th>Types of security breaches experienced in the past 5 years (as % of respondents)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss or theft of device (laptop, USB, hard drive, backup tape)</td>
</tr>
<tr>
<td>Accidental leak of data online</td>
</tr>
<tr>
<td>Intrusion and theft from your IT system</td>
</tr>
<tr>
<td>Hacking/bijacking of social media</td>
</tr>
<tr>
<td>Loss of information from remote data storage systems (cloud computing)</td>
</tr>
<tr>
<td>Other</td>
</tr>
<tr>
<td>We have had no such security breach</td>
</tr>
<tr>
<td>Don’t know</td>
</tr>
</tbody>
</table>

Source: The Economist Intelligence Unit.
With security breaches at Asian companies so prevalent, how are firms working to safeguard the security of their data? What policies do they have in place when things go wrong?

Worryingly, the research shows that nearly a third of businesses do not have a policy in place to deal with the communication of security breaches (Figure 6). This rises to 46% in India, while healthcare firms (53%) and professional services outfits (42%) are the worst industry performers, saying they have no policy for communicating data security breaches.

CSL, a Hong Kong mobile-phone network operator with annual revenues of around US$1bn, is one firm with a data-security policy driven from the top down. It says its data security practice is led by a risk committee, which consists of the CEO and all senior executives. The committee’s job is to manage information risk across the company. All data leaks are reported to the committee. “Any company security initiative which impacts every employee comes directly from the CEO,” says a senior security executive at CSL.

What else should firms be doing to safeguard their data? One option is to combine their efforts with other firms, suppliers and regulators to work together on minimising attacks. Survey responses show that Asian executives and professionals believe in the value of this collaborative approach but are reluctant to act.

Over a third of respondents say they would not reveal to any third party that they had suffered a loss of customer data. However, 47% believe that disclosure can minimise the damage caused by such breaches (Figure 7).

“Keeping silent about an IT attack would be the norm for most companies—it’s the traditional mindset,” says Charles Mok, who represents the IT sector in Hong Kong’s legislative assembly. Even in Hong Kong, with its wired population and modern economy, businesses typically regard IT as a cost, not an investment, Mr Mok believes.

“They still think of it as something to deal with
"Keeping silent about an IT attack would be the norm for most companies—it’s the traditional mindset."

Charles Mok, Legislative Councillor for Information Technology, Hong Kong

My company’s policies do allow for disclosure to external parties, which can have a positive reputational benefit in terms of PR and customer relations. But for a benefit to be felt, companies need to act quickly and transparently.

- Security Chief, Financial Services firm

"If a problem arises. They have not really tried to consider it as an investment or in terms of prevention.”

A significant minority of survey respondents, some 37%, say data security breaches are best dealt with internally. This is especially the case for medium to large companies. Among those with revenue of US$1bn-US$5bn, 56% think that breaches are best dealt with privately. Concerns over sharing private data and fear of reputational harm are the major inhibitors to disclosure across all firm sizes (Figure 8).

The financial services sector regards reputational harm as the biggest obstacle to disclosure, cited by 54%. However, the financial services firm security chief interviewed for this research says, “my company’s policies do allow for disclosure to external parties, which can have a positive

---

### Figure 7: A problem shared...

| Increased disclosure can minimise the damage caused by breaches (% respondents) |
|---------------------------|------------------|------------------|
| Agree                     | 47%              |
| Neither agree nor disagree| 32%              |
| Disagree                  | 17%              |
| Don’t know                | 5%               |

Source: The Economist Intelligence Unit.

### Figure 8: Obstacles exist regardless of size

<table>
<thead>
<tr>
<th>Reasons why our firm doesn’t collaborate (% respondents)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;$500m or less</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No legal requirement</th>
<th>Concerns over sharing private data</th>
<th>Fear of reputational harm</th>
<th>It doesn’t assist in solving the issue</th>
<th>Different data security policies</th>
<th>Incompatible IT systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>80%</td>
<td>70%</td>
<td>60%</td>
<td>50%</td>
<td>40%</td>
<td>30%</td>
</tr>
<tr>
<td>70%</td>
<td>60%</td>
<td>50%</td>
<td>40%</td>
<td>30%</td>
<td>20%</td>
</tr>
<tr>
<td>60%</td>
<td>50%</td>
<td>40%</td>
<td>30%</td>
<td>20%</td>
<td>10%</td>
</tr>
<tr>
<td>50%</td>
<td>40%</td>
<td>30%</td>
<td>20%</td>
<td>10%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Source: The Economist Intelligence Unit.
Sharing the blame: How companies are collaborating on data security breaches

benefit in terms of PR and customer relations. But for a benefit to be felt, companies need to act quickly and transparently.”

The security chief cites a 2008 example from RBS Worldpay, a payment processing company, which had lost data relating to millions of customers. Given the size and extent of the leak, senior management decided the best course of action was to go public with the details. However, the decision to disclose was made 43 days after the incident happened, leading to calls of negligence and ultimately a class action suit against the company.¹

The security chief outlined how RBS Worldpay worked with customers to compensate them for any financial loss and educate them on data security issues. Describing how it also provided customers with credit monitoring facilities for one year. The total cost was a hefty seven-figure sum, as it attempted to make the best of a challenging situation. Ultimately their data security policy was shown to be successful, putting in place significant measures to both protect their customers’ data, and educate them on preventing future breaches.

Research for this report shows that an unwillingness to disclose the loss of customer financial or personal data, particularly to external parties (including the media), is shared by general management in Asia. Perhaps unsurprisingly, executives are significantly less willing to reveal a loss of company data than any other type of breach (Figure 9).

However, senior management and board members are slightly more optimistic than others about the benefits of disclosure. A majority of CEOs, CIOs and board members feel that there is a benefit to disclosing to customers a breach in

¹ Class action complaint v. RBS Worldpay Inc http://datalossdb.org/attachments/0000/0423/RBS_complaint.pdf
their data (Figure 10). CFOs, along with the rest of management, appear more sceptical about the benefits of disclosure to customers. Across all firms, no one would consider disclosing instances involving a breach of customer information to the media or competitors.

The highest level of collaboration is in the financial services sector. Only 11% of financial services firms do not collaborate with any third parties on data security, compared to an average across Asia of 23%. Their preferred partners are IT vendors (chosen by 76%) and law firms (35%), who are also the first two choices of respondents as a whole (61% and 29% respectively—Figure 11).

Government regulation increasingly influences the disclosure practices of many firms, significantly those within the financial services sector where they often have a legal obligation to disclose breaches. However, reputation management also plays a role, with a firm’s desire to collaborate sometimes driven by the media attention that any form of breach generates, irrespective of where the security fault occurs.

In December 2013 Singapore police disclosed to the media that personal banking information had been stolen from a third-party contractor to Standard Chartered Bank. The contractor, Fuji Xerox, had been hired to print bank statements on behalf of the bank and had not disclosed the theft. According to the bank the theft of the bank statements did not occur through its IT and data security systems.2 Regardless, the incident caused the bank reputational damage from negative press coverage and regulatory penalties that closer collaboration with its supplier may have avoided. In April 2014, the Monetary Authority of Singapore announced they had taken appropriate supervisory actions against the bank.3

---

2 http://www.ft.com/intl/cms/s/0/56422a0c-c162-11e3-97b2-00144feabdc0.html#axzz30nqJsJ4v

The financial services firm security chief says banks are increasingly collaborating over data security breaches, in both informal and formal ways. For example, Chief Security Officers (CSOs) and security staff talk to each other in informal working groups on data security issues. At a formal level, US banks have worked together to respond to specific cyber attacks, sharing information on the nature of the threats.

Another approach to help banks is offered by non-profits such as Financial Services Information Sharing and Analysis Centre (FSISAC), whose website (www.fsisac.com) allows organisations to disclose data anonymously.
The survey shows that there is broad agreement about the benefits of disclosure as a weapon against breaches, in particular that it would improve the perception of data security (a view with which about 57% agree). Nearly half also recognise the benefit of disclosure in minimising the damage or reputational harm caused by breaches (Figure 12). Customer relations staff are the most positive about the impact of disclosure, polling ahead of the overall average in every case.

A separate global research report on information risk published by The Economist Intelligence Unit in November 2013 says sharing knowledge of threats is one of the critical steps in improving information risk management. It is much more effective to share knowledge with competitors and peers rather than waiting for the government or others to act.

The senior security executive from CSL says the company believes in transparency as a means of advancing information security. “The less transparent you are, the less the likelihood that you will find the answer. CSL is not scared about disclosing security breaches, and we follow the regulatory requirements.”

---

That said, CSL’s disclosure is limited to reporting customer data breaches to the telecommunications industry regulator, Ofca, and the Hong Kong Privacy Commissioner Office, as required by law. It doesn’t disclose data breaches to its competitors, although the senior executive says it has shared information regarding breaches with one of its suppliers.

More than 70% of respondents agree that it is impossible to prevent all data breaches, and thus the way they are handled is important (Figure 13).

![Figure 13: A Sisyphean task?](image)

Increasing the importance of data security means that “you can’t just leave it to the IT guys, especially when it comes to privacy. And even if the IT group knows what to do, the CMO may complain.”

Charles Mok, Legislative Councillor for Information Technology, Hong Kong

However, the EIU Information Risk paper warns that businesses are failing to create a culture of awareness around data risk. Just 27% of companies in that paper report an extensive awareness of information risk across the organisation. Outside the IT and finance departments, the importance of protecting data has not filtered across the organisation or down to the lower levels.

At the same time, business leaders appear ill-prepared for a loss of information at their company. The survey reveals that fewer than a quarter would know enough to take the lead in the event of a breach, despite nearly half of organisations experiencing a loss of information in the past two years.

Mr Mok, the Hong Kong legislator, says the increasing importance of data security means that “you can’t just leave it to the IT guys, especially when it comes to privacy. And even if the IT group knows what to do, the CMO may complain.”

He says that as well as creating company-wide policies, organisations need a CSO to oversee security and privacy.

With security breaches on the rise, all companies need to consider the best way of minimising their
Sharing the blame: How companies are collaborating on data security breaches

impact. Asked how they would avoid future data breaches, just 34% of companies say they would consider a review of disclosure policies, while 27% might build closer ties with third parties (Figure 14).

These numbers indicate a surprisingly gloomy outlook, with an acceptance of high levels of data breaches yet very little appetite for making changes to disclosure practices. This is true of companies of all sizes. Even among those most willing to consider disclosure—firms with over US$10bn revenue and those with revenues of between US$500m and $1bn—the level of support is below 50%.

The financial services security head believes regulation can help. He says the Monetary Authority of Singapore (MAS) has been effective in using relatively small fines to force compliance. But the biggest factor is companies wanting to minimise the reputational damage that breaches can cause.

Survey respondents are united in agreeing that companies must take the lead in protecting data security. Some 82% say that business must proactively take the initiative in ensuring data security. Only 5% disagree (Figure 15). Among financial services firms, 92% agree.

The 2013 Information Risk study by the EIU found that most executives believe governments and regulators can play a role in facilitating a company’s collaboration and knowledge sharing. Over three-fifths of respondents in that study (62%) said governments should take a greater lead in information risk management, particularly by encouraging knowledge sharing between companies about cyber-attacks. They are advocating co-operation, not necessarily legislation. An even larger proportion (68%) of respondents called for greater regional harmonisation of the rules surrounding data security.

Mr Mok emphasises that business, not government, must take the lead in managing breaches and creating awareness of their danger. “I know it’s difficult. But there is no clear example of good government regulation to enforce cyber security.”
Conclusion

Companies in Asia, as in the rest of the world, face significant challenges when trying to securely manage data. Trusted security systems are being routinely breached, while government regulation of cyber security is often found wanting, creating an environment where managers now expect some data to be lost.

When faced with these challenges, however, managers remain upbeat about their efforts to safeguard the security of customer data. They recognise that IT systems will be breached, but through constant monitoring of policies and procedures, they are confident of limiting the damage caused. Significantly, they also recognise the advantages of collaborating with other industry stakeholders (media and competitors excepted) to coordinate their response to attacks.

Security breaches, unlike government policy, are not restricted by country borders but can rapidly spread across the globe, as the recent Heartbleed bug outbreak so alarmingly showed. Hence, in order for firms to minimise the damage data loss can cause, they need to take the lead in preventing breaches both within their organisation and through collaborating with others across the region. The public still has a high level of trust in the way firms handle their data, but if the number and severity of security breaches increases then it won’t be long before the public is blaming someone for the damage they cause.
While every effort has been taken to verify the accuracy of this information, The Economist Intelligence Unit Ltd. cannot accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in this report.
LONDON
20 Cabot Square
London
E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8500
E-mail: london@eiu.com

NEW YORK
750 Third Avenue
5th Floor
New York, NY 10017, US
Tel: (1.212) 554 0600
Fax: (1.212) 586 0248
E-mail: newyork@eiu.com

GENEVA
Rue de l’Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 9347
E-mail: geneva@eiu.com

HONG KONG
6001, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com

SINGAPORE
No. 8 Cross Street
#23-01 PWC Building, 048424
Singapore
Tel: (65) 6534 5177
Fax: (65) 6534 5077
E-mail: asia@eiu.com