VeriSign®
A SYMANTEC AFFILIATED COMPANY

IDG Connect, a division of International Data Group (IDG), the world's largest technology media company, produces, publishes and distributes local IT and business information on behalf of a truly global client base. Established in 2005, we have a fully nurtured audience of 2.6 million professional decision-makers from 130 countries, and an extended reach of 38 million names. This lets us conduct research, create independent analysis and opinion articles, and drive long-term engagement between professionals and B2B marketers worldwide. For more information visit: www.idgconnectmarketers.com

IDG CONNECT

Online and At Risk

Japan: Vulnerabilities in Website Security

Survey conducted by IDG Connect on behalf of Verisign

VeriSign®
A SYMANTEC AFFILIATED COMPANY

IDG Connect, a division of International Data Group (IDG), the world's largest technology media company, produces, publishes and distributes local IT and business information on behalf of a truly global client base. Established in 2005, we have a fully nurtured audience of 2.6 million professional decision-makers from 130 countries, and an extended reach of 38 million names. This lets us conduct research, create independent analysis and opinion articles, and drive long-term engagement between professionals and B2B marketers worldwide. For more information visit: www.idgconnectmarketers.com

IDG CONNECT

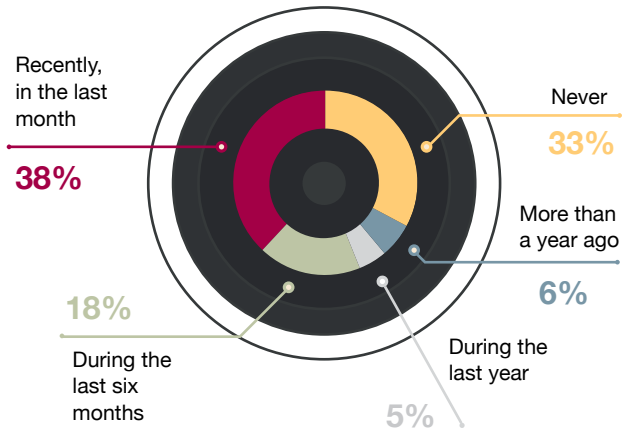
Between Words and Actions: The Vulnerability Gap

The effects of the world's largest ever data breach – caused by an attack on a Japanese electronics company in 2011 – are still being felt. The intrusion, which resulted in the leakage of 77m customer account records, appears to have exploited a failure to apply updates to Apache web servers. Nearly two years later, the fallout continues to rain down: in North America and Europe, the company in question remains embroiled in lawsuits and disputes with data protection regulators.

Corporates often talk a good game when it comes to website security. But they frequently test and protect their sites less rigorously than their rhetoric suggests. In previous surveys of IT professionals in Europe and US, we have described this distance between words and actions as a vulnerability gap.

Our research suggests that complacency and denial often flourish in the vulnerability gap. But are Japanese companies putting themselves at risk in the same ways as their counterparts in Europe and North America? To find out, in March 2013 we surveyed 100 senior IT executives in small, medium and large Japanese enterprises.*

When did you last conduct a vulnerability assessment/ scan on your website(s)?



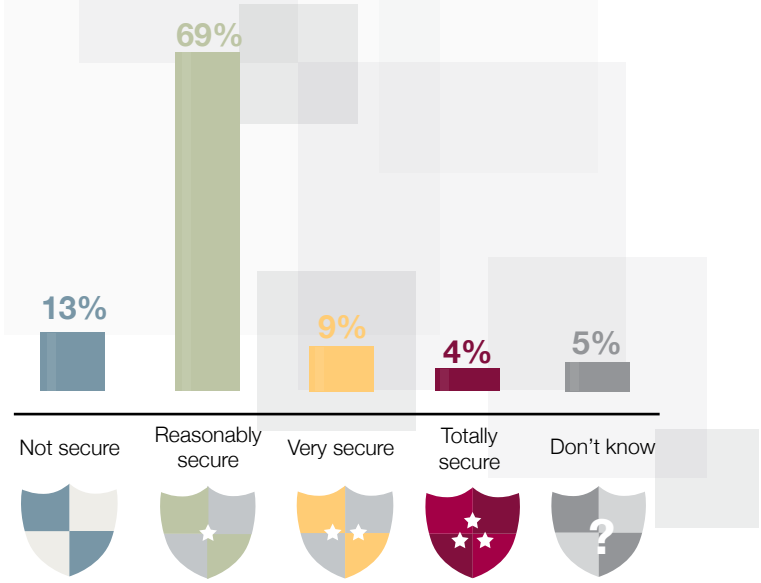
The results suggest that – despite some significant differences in approach – a substantial number of Japanese companies are failing to address acknowledged vulnerabilities in their web-based operations.

Three out of five Japanese companies qualify as risk-takers who have never tested their sites for vulnerabilities or who last did so over a year ago. However, if you merely listened to the words of Japanese corporates, you would never suspect this. Only one in five say they don't know how secure their sites are, or that their sites are "not secure".

Corporate Japan appears to be taking substantial risks with internet security. As attacks increase in number and sophistication, the gap between words and actions is becoming increasingly problematic.

* Survey conducted by IDG Connect on behalf of Symantec in March 2013. In October 2012, identical surveys were conducted among 100 respondents apiece in North America and Europe (France, Germany, Sweden and the UK)

How secure do you consider your website(s) to be?



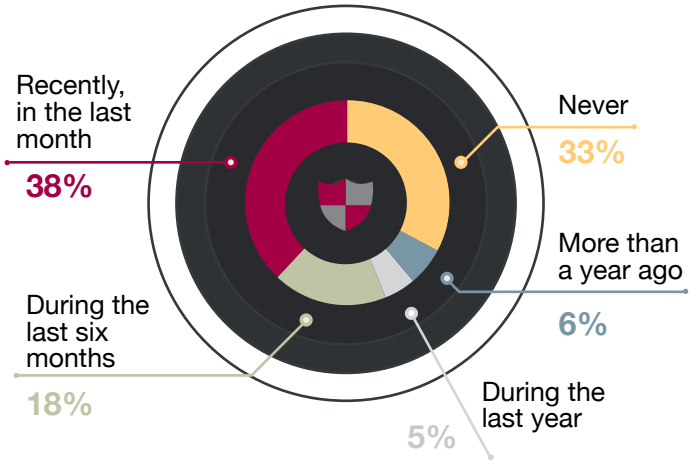
VeriSign®
A SYMANTEC AFFILIATED COMPANY

IDG Connect, a division of International Data Group (IDG), the world's largest technology media company, produces, publishes and distributes local IT and business information on behalf of a truly global client base. Established in 2005, we have a fully nurtured audience of 2.6 million professional decision-makers from 130 countries, and an extended reach of 38 million names. This lets us conduct research, create independent analysis and opinion articles, and drive long-term engagement between professionals and B2B marketers worldwide. For more information visit: www.idgconnectmarketers.com

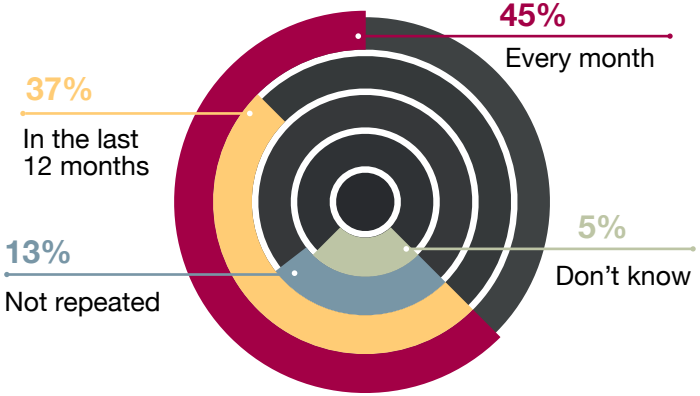
IDG CONNECT

Website Security in Japan: How Big Are the Risks?

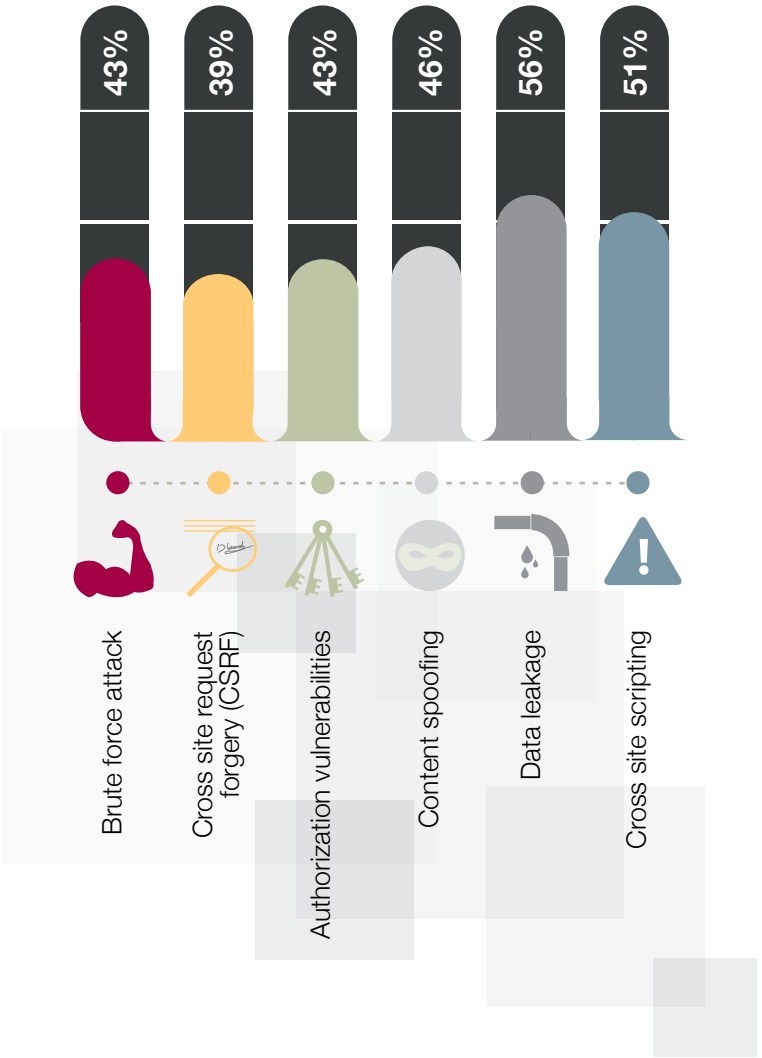
When did you last conduct a vulnerability assessment/ scan on your website(s)?



How often have you repeated vulnerability assessments on your website(s)?



It is likely or very likely that our website(s) suffer from the following vulnerabilities:



VeriSign®
A SYMANTEC AFFILIATED COMPANY

IDG Connect, a division of International Data Group (IDG), the world's largest technology media company, produces, publishes and distributes local IT and business information on behalf of a truly global client base. Established in 2005, we have a fully nurtured audience of 2.6 million professional decision-makers from 130 countries, and an extended reach of 38 million names. This lets us conduct research, create independent analysis and opinion articles, and drive long-term engagement between professionals and B2B marketers worldwide. For more information visit: www.idgconnectmarketers.com

IDG CONNECT

Reasonably Secure: Are IT Managers Realistic Or In Denial?

Japanese IT executives are significantly less likely than their counterparts in Europe and North America to describe their website(s) as "totally" or "very" secure. They're more likely to admit that their site(s) are not secure, or merely "reasonably secure".

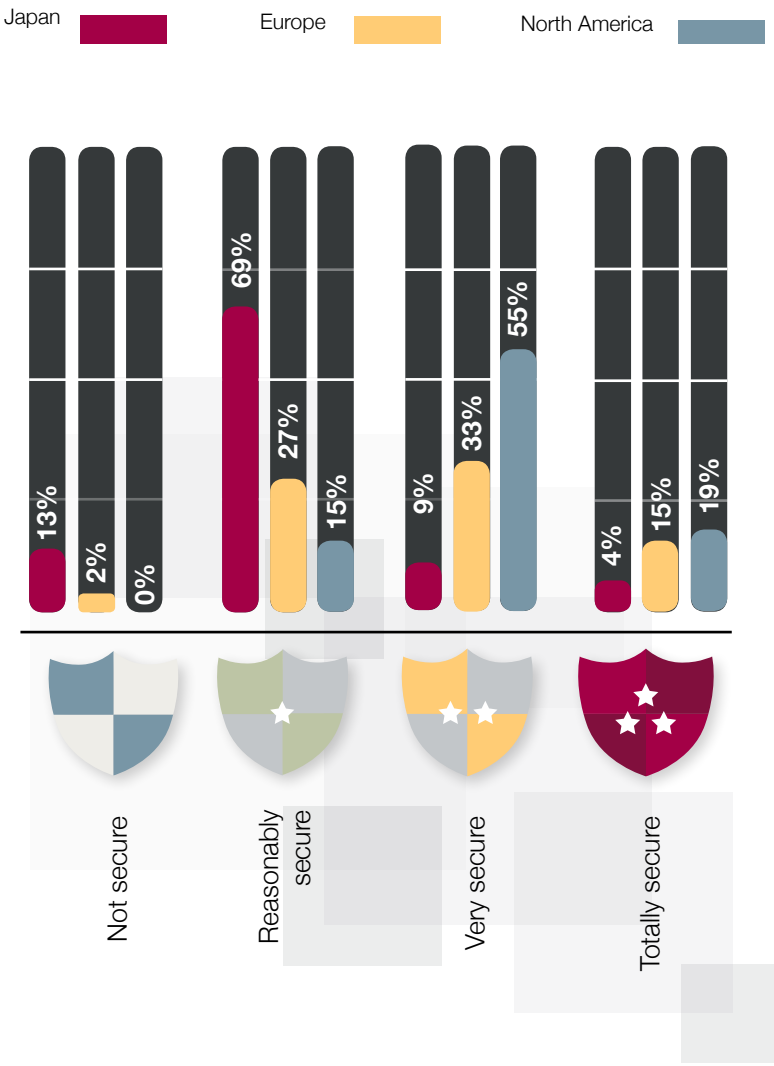
In our previous analysis of survey results in Europe and North America, we described some IT executives' approach to web-based security as being underwritten by "baseless optimism". The results of this survey suggest that Japanese IT executives are more realistic, perhaps informed by superior understanding of web-based threats (only 5% replied "don't know" when asked about the security of their sites, compared with 23% in Europe and 11% in North America). However, the very pronounced tendency for Japanese respondents to describe their website(s) as "reasonably secure" raises the question: what is reasonable?

Here, it's helpful to measure words against actions. Despite their apparently more realistic stance, Japanese companies follow a pattern that's very similar to American companies when it comes to frequency of vulnerability assessments. For example, 38% had tested for weaknesses during the past month, versus 41% of North American companies we surveyed.

Indeed, an identical proportion of respondents in North America and Japan (13%) told us that they were aware of an internet security breach at their organisation during the past six months. Despite the apparent realism of Japanese IT executives, the corporate sites they oversee appear to be just as vulnerable to attack as those in North America.

"Reasonably secure" sounds positive – and measured. But our detailed findings suggest that it's worth interpreting the public assessments of IT executives cautiously. Many of the corporate websites described by Japanese IT executives as "reasonably secure" may, in fact, suffer from significant security weaknesses.

How secure do you consider your website(s) to be?



VeriSign®
A SYMANTEC AFFILIATED COMPANY

Infrequent Audits

Securing corporate websites isn't a one-time job. It's a continuous process. In the absence of frequent vulnerability testing, companies open themselves up to breaches that can go undetected for long periods of time.

Only 67% of our survey respondents had ever conducted a vulnerability assessment on their website(s). We asked these respondents how often they had repeated the exercise.

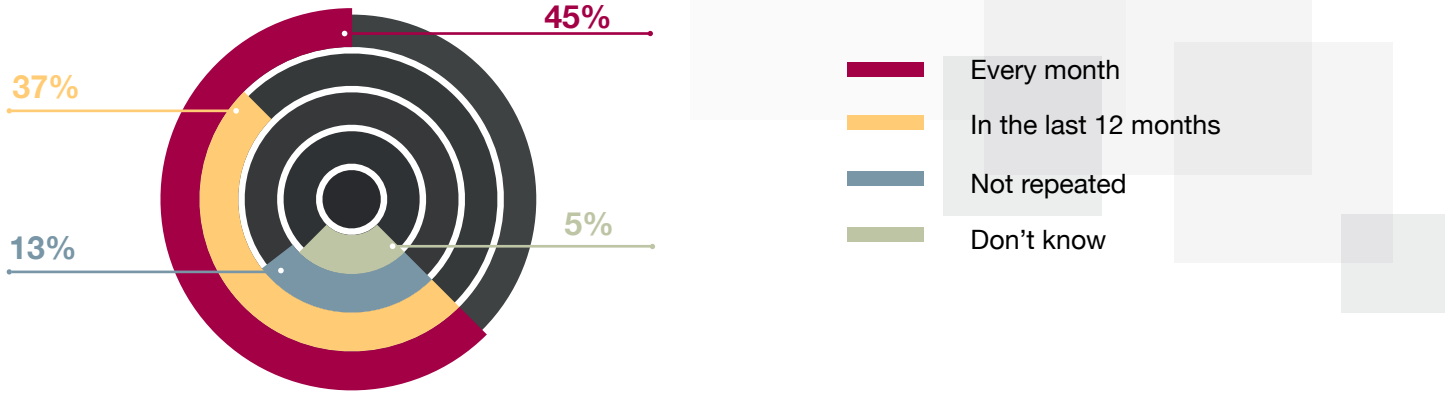
Here, a sharp divide opened up between those who conduct monthly assessments (45%) and those whose testing regime is much more relaxed, with up to a year stretching between assessments (37%).

This finding and others in our survey suggest that Japanese companies fall into three broad groups:

- Pro-active vulnerability testers: At the time of our survey, these companies had tested for vulnerabilities in the past month, as part of a continuous monthly testing regime.
- Sporadic testers: Those whose most recent test occurred between 1 and 12 months ago, and whose testing regime is haphazard in terms of frequency.
- Do-nothing laggards: 33% told us they had never tested for vulnerabilities. In addition, 9% of our survey sample told us they had only ever performed a single vulnerability assessment and never repeated it.

For the last group in particular, which comprises almost half of Japanese companies we surveyed, the outlook is worrying. Their lack of even routine analysis leaves them exposed to substantial threats, and the consequent risk of reputational and financial damage from a serious security breach.

How often have you repeated vulnerability assessments on your website(s)?



VeriSign®
A SYMANTEC AFFILIATED COMPANY

Threats Emerging From All Angles

A vulnerability is any potential entry point through which a website's functionality or data can be damaged, downloaded, or manipulated.

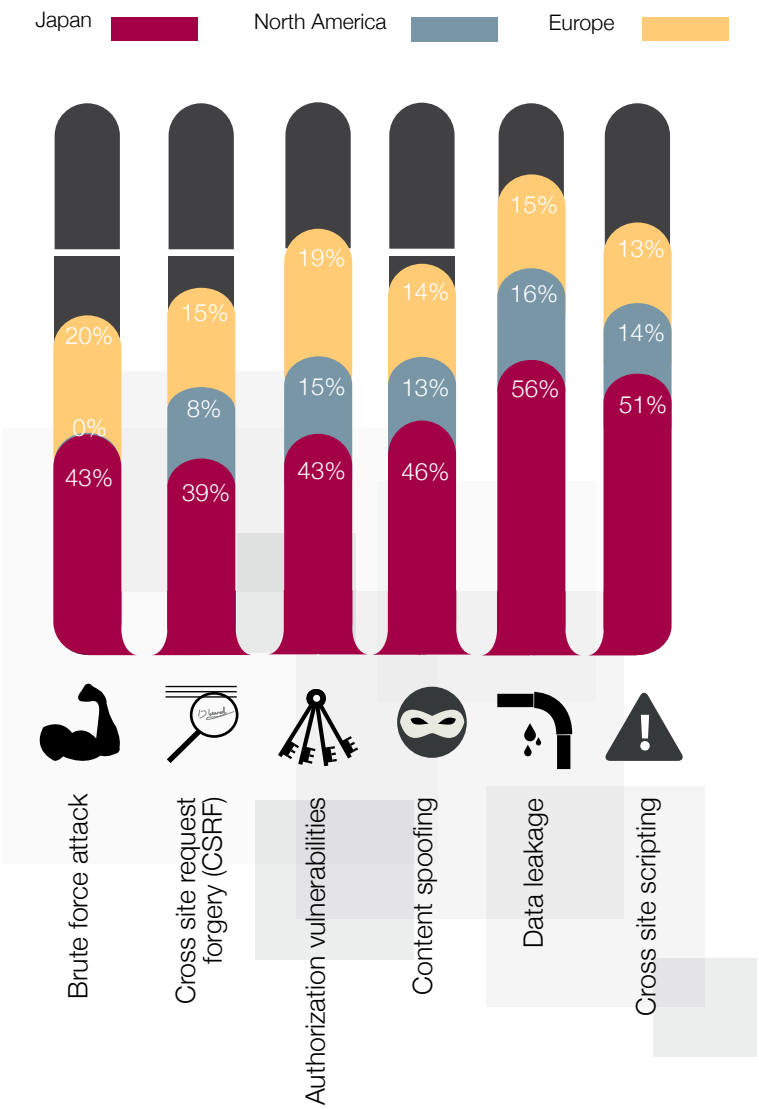
Websites can have many potential vulnerabilities, and cybercriminals play an odds-based game. In the weeks running up to a major breach, for example, it's not unusual for a company's servers to suffer massive denial of service (DDoS) attacks, which are designed to sniff out an entry point and vulnerabilities ripe for exploitation.

Our Japanese respondents identified data leakage and cross-site scripting as the attack vectors to which their sites are most vulnerable. However, the threats posed by these weaknesses are not seen as substantially greater than other threats. In the view of most respondents, danger lurks everywhere and challenges come from all angles. The wide variety of perceived threats underlines the risks firms undertake when they don't check regularly for vulnerabilities and adhere to security best practice.

Notably, Japanese IT executives are far more likely to admit that their sites are likely (or very likely) to suffer from the specific vulnerabilities we described than their counterparts in Europe and the US. Depending upon your perspective, you might describe this – once again – as realism. Alternatively, you might describe it as a clear admission of weakness caused by poor security procedures.

The fact that a large minority of Japanese companies test their websites infrequently (or not at all) may well be what causes a similarly-sized number of respondents to say that their site(s) are likely or very likely to suffer from multiple vulnerabilities.

It is likely or very likely that our website(s) suffer from the following vulnerabilities



VeriSign®
A SYMANTEC AFFILIATED COMPANY

IDG Connect, a division of International Data Group (IDG), the world's largest technology media company, produces, publishes and distributes local IT and business information on behalf of a truly global client base. Established in 2005, we have a fully nurtured audience of 2.6 million professional decision-makers from 130 countries, and an extended reach of 38 million names. This lets us conduct research, create independent analysis and opinion articles, and drive long-term engagement between professionals and B2B marketers worldwide. For more information visit: www.idgconnectmarketers.com

IDG CONNECT

One in Eight Companies Breached in the Past Six Months

A significant number (13%) of Japanese companies told us they had suffered a breach of internet security during the past six months.

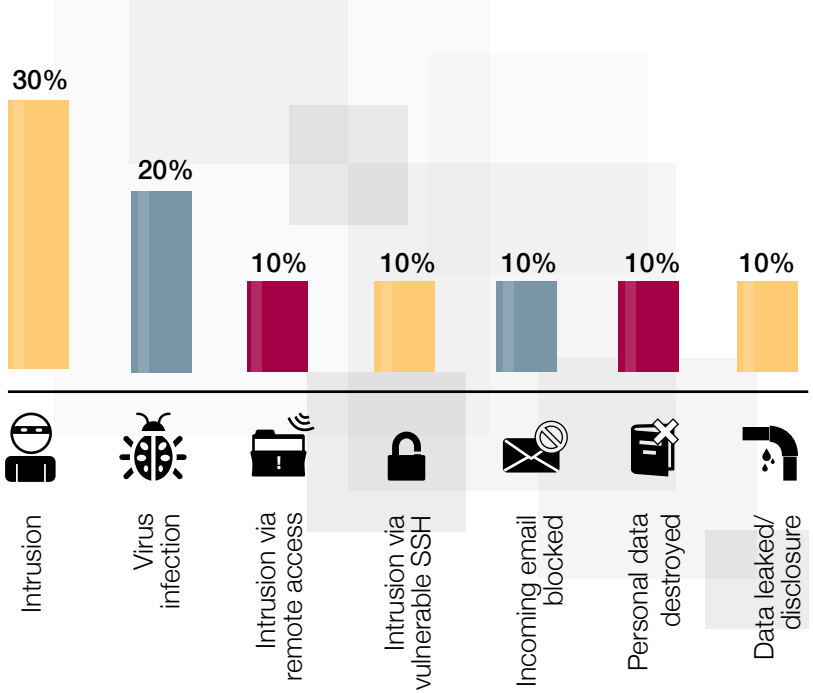
The numbers show that internet security challenges constitute a genuine threat. The maths suggests that in any given year, one-quarter of Japanese companies will find their web security compromised. Over a four year period, most, if not all, Japanese companies will suffer some kind of internet security breach.

Asked the same question in late 2012, 13% of North American respondents and 9% of European respondents confirmed the existence of breaches during the most recent six month period. Our survey data confirms what the known activities of cybercriminal gangs suggest: that security threats are evenly distributed globally.

The sheer variety of compromises regarded as most serious by Japanese companies that have suffered attacks is striking. At a deeper level, the security breaches regarded as most serious fall into two categories: breaches that resulted in destruction or direct economic damage (incoming email blocked, personal data destroyed, for example) and those associated with intrusion. Worryingly, the true cost of the latter may never be known.

Are you aware of any internet security breaches within your organisation in the last six months?

If you are aware of one or more breaches of internet security during the past six months, please provide an example of the most serious breach that occurred.



Significant Outcomes

Of the security breaches experienced by Japanese companies during the past six months, 62% resulted in some kind of disruptive impact. (This may well be an underestimate. Respondents could be minimising the impact of some breaches; alternatively, the impact of "harmless" security breaches may, in fact, have gone undetected.)

Only 1 out of 100 respondents told us that their company had suffered an internet security breach during the past six months that resulted in a major impact, such as the leaking of customer data.

This seems, at first glance, a small number. But it's important to understand the implications: first, at the level of the Japanese economy as a whole, and second, in terms of the potential impact if your company suffers a serious breach. Some 3,900 companies are listed on the Japanese stock exchange, with an aggregate market capitalisation of US$3.7 trillion [(1)]. In total, the Japanese economy comprises 4.2m enterprises of all sizes [(2)]. Taken at face value, these figures suggest that up to one million Japanese companies are successfully breached every year.

It's true, of course, that not all of these companies maintain customer-facing websites that process user data. But many do. Here's just one statistic among many that suggest the scale of the risk involved: in 2012, Japanese companies processed $128bn-worth of online orders. The vast majority of these orders were placed by 73m Japanese consumers who buy goods and services online [(3)].

For companies hit by a major breach, the stakes are high. Like any business, cybercriminal gangs have a tendency to prefer multiple revenue streams: they may profit by selling stolen customer information, source code and confidential corporate data. They may also seek to benefit by compromising your servers and using them to infect your users' computers. It's not unusual for sophisticated breaches to go undetected in the background for long periods.

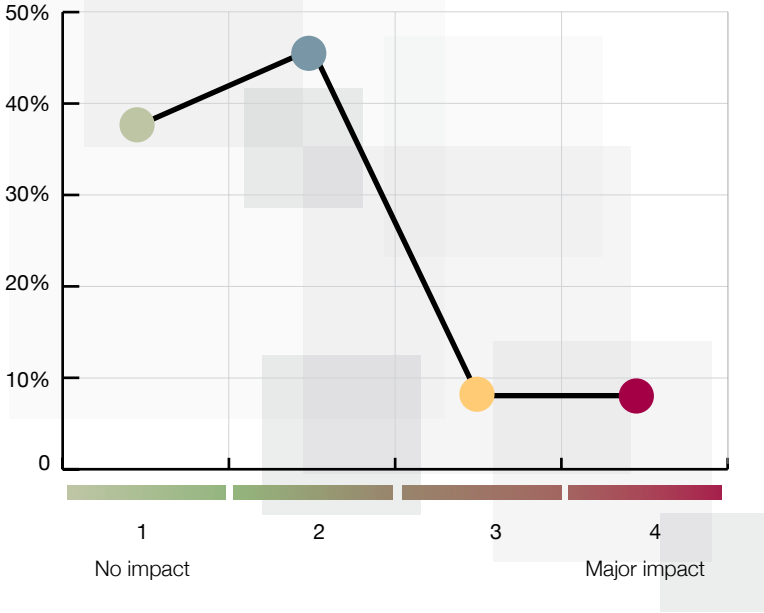
The cost of security breaches can be substantial. In addition to the cost of investigating the problem and rectifying it, companies often have to deal with a loss of confidence among investors, long-term brand damage, class action lawsuits and fines levied by data protection authorities at home and overseas.

(1) World bank

(2) Japan Small Business Research Institute

(3) eMarketer, Ecommerce sales topped $1 trillion for first time in 2012 (February 2013)

How disruptive was the breach?



Protective Measures

Recovering from a security breach can be a lengthy process. Diagnosing the original vulnerability often involves pain-staking forensic investigation. According to research conducted by the Ponemon Institute on behalf of Symantec, the average cost of a data breach among a selection of 51 US companies in 2010 was US$7.2m.

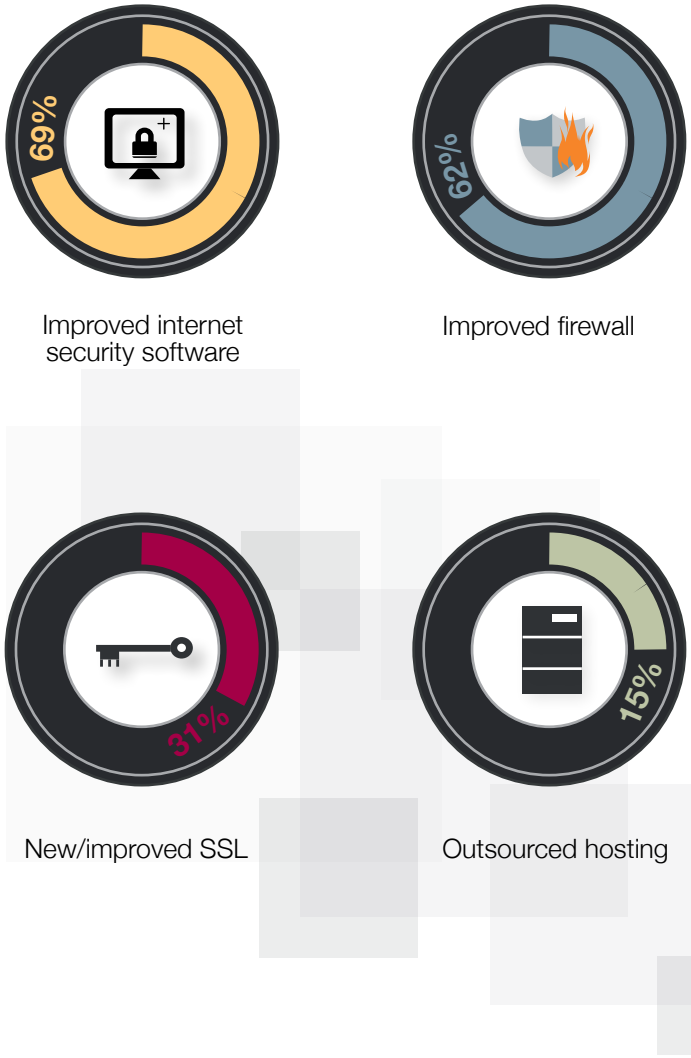
In addition, the job of patching or rewriting code in order to get systems running again has to be accomplished as soon as possible, in order to minimise revenue loss. This typically involves large unbudgeted costs as IT staff attempt to compensate for past errors and omissions. Other risks lurk in the undergrowth, including the possibility that attackers will assume that similar weaknesses exist elsewhere across your web estate. Shortly after the May 2011 incident in which a well-known Japanese electronics company suffered its first huge data breach, for example, the same company's servers in Europe and Russia were subjected to a separate wave of attacks. This isn't unusual: one of the side effects of a successful exploit is a surge of copycat attacks, which use similar techniques to try to exploit similar vulnerabilities.

Longer term, the most common responses of Japanese companies who told us they had been breached included battening down the hatches with upgraded security software and firewalls.

A significant minority are turning to third-parties in order to gain access to expertise and reduce the administrative burden of security. As enterprises turn increasingly to the Cloud, it seems likely that third party solutions of this kind will become increasingly accepted in enterprises. In the context of multiple attack possibilities (see Recent Breaches tab) and zero day exploits, the tendency to rely upon outside expertise is entirely understandable [4].

(4) Leyla Bilge, Tudor Dumitras, Before We Knew It: An Empirical Study of Zero-Day Attacks In the Real World (Symantec Research Labs, October 2012)

Tactics for combating future threats



Security Hygiene

Companies that conduct remote scans – more than half of the companies we surveyed – are 1.5 times more likely to conduct monthly security assessments, thereby increasing their chances of remaining secure.

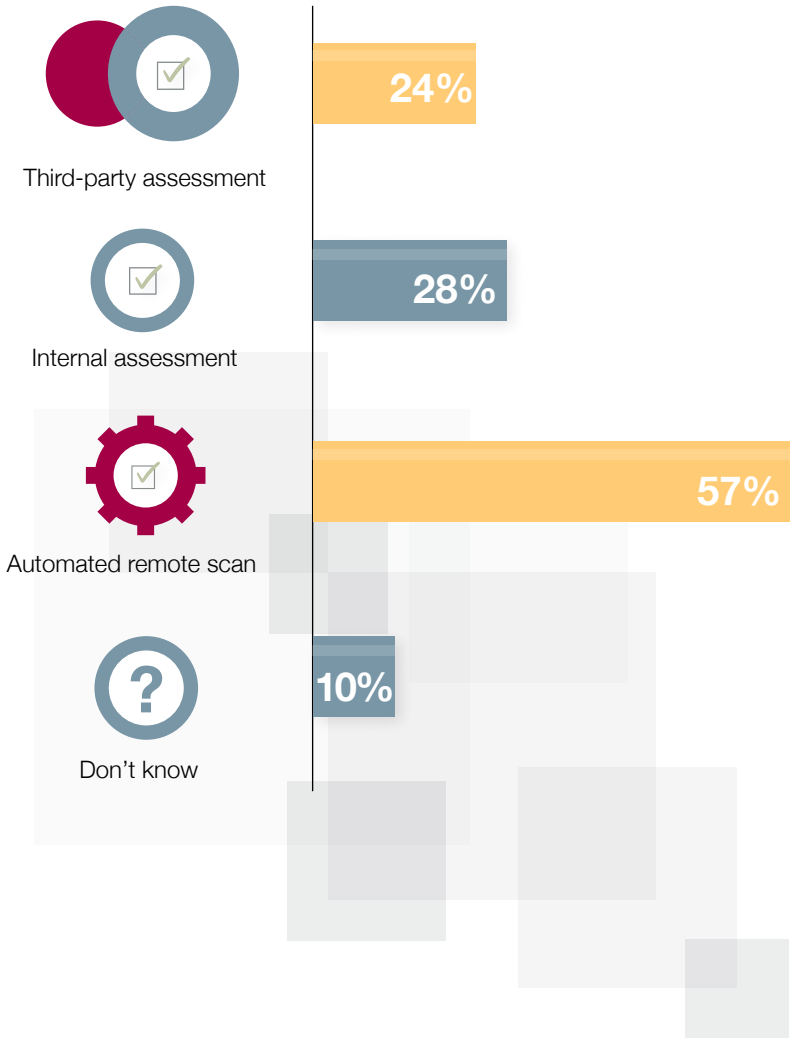
There are two likely explanations for this. It may be the case that companies running remote scans are by their nature more security conscious. This alone may explain their tendency to scan more frequently than others. But there's another possible explanation: assessments of vulnerability undertaken by internal staff tend to be labour-intensive, and may involve depriving other projects of resources. This may well explain why companies that use automated scans are able to check for vulnerabilities more frequently.

Given a rapidly changing threat landscape, the economies of scale inherent in automated scanning make a lot of sense: with the collective intelligence of a third-party security provider embodied in software, IT managers can decide when and where further investigation by internal and/or external teams is required.

Japanese companies have adopted remote automated scanning in an aggressive fashion. While 57% of Japanese companies use automated remote scanning, only 18% of companies in North America, and 6% in Europe do so. In both North America and Europe, reliance on internal assessments is much higher. Use of third-party assessments is also significantly higher in Europe than in Japan.

Notably, 62% of companies who suffered breaches told us that they subsequently put in place improved firewall protection. In this respect, Symantec Japan can help: its Web Application Firewall (WAF) allows the setting of parameters to combat incoming threats and is regularly updated with new signatures that seek out novel threats. WAF also minimises the need for downtime by working seamlessly in the Cloud with your web assets. The result is enhanced up-to-date protection, with the minimum of disruption.

Vulnerability assessment methods



VeriSign®
A SYMANTEC AFFILIATED COMPANY

IDG Connect, a division of International Data Group (IDG), the world's largest technology media company, produces, publishes and distributes local IT and business information on behalf of a truly global client base. Established in 2005, we have a fully nurtured audience of 2.6 million professional decision-makers from 130 countries, and an extended reach of 38 million names. This lets us conduct research, create independent analysis and opinion articles, and drive long-term engagement between professionals and B2B marketers worldwide. For more information visit: www.idgconnectmarketers.com

IDG CONNECT

Scan Often, Scan Regularly

A large majority of Japanese companies describe their websites as "reasonably secure". While this verdict seems reassuring, there's a caveat. Our research indicates that a significant minority of Japanese companies have never assessed their sites' vulnerabilities (33%), or have only ever done so once (9%).

For these companies, many of whom told us their sites are "reasonably secure", the vulnerability gap looms large. Within it, complacency and denial take root. Notably, Japanese IT executives are much more willing to accept the likelihood of vulnerability to specific exploits than their counterparts in Europe and North America. This suggests that in Japan, denial is more of a challenge than complacency.

However, this survey also offers evidence for optimism. Japanese companies have adopted remote automated scanning enthusiastically. Our research suggests that companies using remote scanning are 1.5 times more likely to conduct vulnerability assessments on a monthly basis.

The more Japanese companies adopt remote scanning, the better their levels of protection will become. Symantec offers a range of solutions, including free weekly automated scans identifying critical vulnerabilities for customers who use Symantec Secure Site Pro With EV, Secure Site With EV and Secure Site Pro SSL Certificates [5].

The stakes are substantial. The new generation of so-called Advanced Persistent Threats (e.g. stuxnet) are not only a way of sabotaging, or extracting intelligence from, governments and large companies in strategically important industries. Frequently, the basic motivation is economic and criminal. The range of organisations at risk is correspondingly wide.

The vast majority of companies that undertake web-based operations own and process data. This makes them vulnerable to theft undertaken by intruders intent on illicitly monetising that data.

Our research suggests that up to a quarter of Japanese companies suffer a security breach every year. We suggest caution when interpreting respondents' suggestion that four in ten of these breaches had "no impact". At the very least, even "harmless" breaches trigger costly efforts to establish how, when, where and why the breach occurred. There are also the costs of remedial action to consider.

Breaches resulting in a major impact seem relatively rare. (This survey suggests that over 2% of Japanese companies fall victim to a major breach of every year.) However, the costs can be substantial, and the long-term impact can be severe. Across the Japanese economy as a whole, the cost of internet security breaches is real and substantial.

The approach of Japanese companies that remain complacent or in denial is deeply problematic. Neither consumers nor shareholders can easily tell whether an organisation has weak security policies. Both can end up as victims of an approach to security risk of which they were never aware, and to which they didn't consent.

5) For further information: http://www.symantec.com/theme.jsp?themeid=ssl-resources#includes_vulnerability_assessment