



e-crime

SURVEY

2009

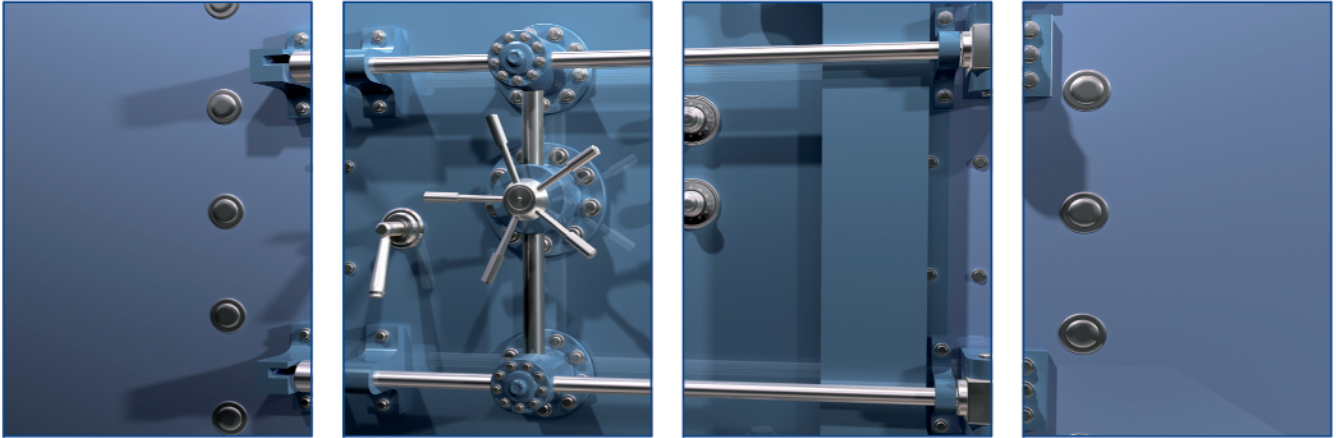
Conducted by

The 7th Annual e-Crime Congress

in partnership with



Established track record Timely international response Tailored range of services



KPMG member firms can help.

As one of the world's leading providers of Information Protection and Forensic advice, KPMG firms can help you to effectively assess and respond to your e-Crime risks.

With a wealth of experience, we know how to help clients protect their information assets, to counter increased risks and address the concerns of customers and regulators.

Security assessment and assurance

Understanding where you are vulnerable is critical to actively managing the risks you face, and reducing the threat from electronic crime.

We can help you understand and identify weaknesses in your information handling systems and processes. Our services range from in-depth technical reviews of IT systems to external and internal penetration tests, as well as evaluations of governance and policy arrangements.

To find out more, contact

**Malcolm Marshall from
KPMG in the UK**
+44 (0) 20 7311 5456
malcolm.marshall@kpmg.co.uk

Forensic response and incident management

Where an e-Crime incident is suspected or has taken place, an immediate and decisive response is essential.

We can help you to secure evidence, assess impact of security breaches and implement recovery strategies. We also help you to work with relevant authorities and regulators, and collaborate with legal advisers. Furthermore, we can investigate any resulting theft of information or fraudulent actions against the business.

To find out more, contact

**Paul Tombleson from KPMG
in the UK**
+44 (0) 20 7311 3964
paul.tombleson@kpmg.co.uk
kpmg.com/forensic

Contents

Overview	3
Executive summary	4
From the editor	6
Key findings	7
On the recession	7
On fraud	10
Online consumer security	16
On e-Crime and enterprise defence	19
Attack trends: the network	19
Attack trends: the web gateway	20
e-Crime defence	21
Protecting the infrastructure	22
Malware	24
On cyber defence and critical national infrastructure	26
On the business of security	29
Mind the gap	29
Spending trends	30
The PCI DSS	31
Governance and proportionate security	32
Summary and conclusions	36
Postscript	37
Contact details	38

Overview

Prior to the 7th annual e-Crime Congress, security professionals from the e-Crime community and a selected group of KPMG's clients were invited to participate in the e-Crime Survey 2009.

The survey was conducted with the aim of stimulating conversation and debate at the Congress on a range of topics with direct relevance to the phenomenon of electronic and Internet-based crime. Between the 3rd February and the 13th March, 307 respondents from global businesses, law enforcement agencies, and government completed the survey.

Individuals who took part represent a cross-section of strategic and operational disciplines including IT security, fraud investigations, corporate security, audit, and risk. They share the commonality of being directly responsible for defending against e-Crime as it affects their organisations and their customers.

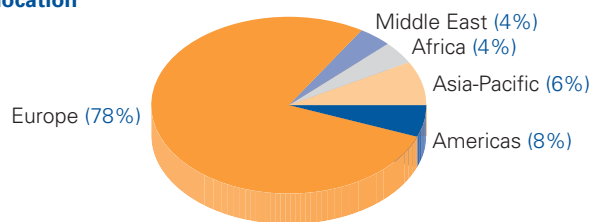
The majority of respondents (80%) work in the private sector, and the results of the survey represent a spectrum of opinions from those in industries that include Financial Services, Retail, Telecommunications, Oil and Gas, Utilities, Gambling, Manufacturing, Media, Transport and Logistics.

This report highlights the most thought-provoking trends revealed by the results. It also presents selected views and opinions from respondents that reflect the experiences of those "at the coal face" of attack detection and threat prevention. These can be seen in sections headed "From the frontlines..."

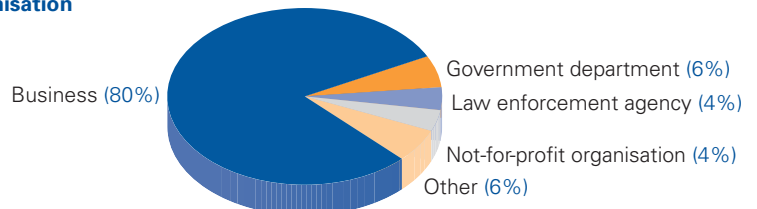
Survey data is presented in aggregate. Respondent's comments are non-attributable.

Key demographic data

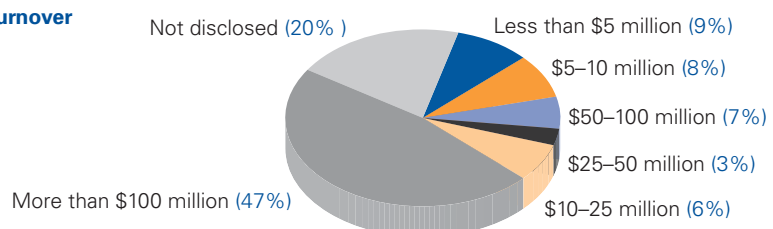
Respondents' location



Type of organisation



Turnover



Executive summary

Clouds are gathering on the horizon...

79% of survey respondents do not believe that security software based on signature detection offers a sufficient level of protection to Internet users.

50% of respondents from IT security do not believe their organisation is sufficiently protected against malware when considering internal Internet usage trends, attack vectors, potential targets, security update procedures, and the risks associated with compromise to their business.

62% of respondents do not believe their business dedicates enough time, budget and resources to locating vulnerabilities.

66% of respondents agree that an increase in out-of-work IT professionals during the recession will lead to more people with technical skills joining the cyber-criminal underground economy.

The arms race is gathering pace...

41% of respondents have indicated an increase in the technical sophistication of attacks on their network.

45% of respondents indicated an increase in phishing targeting employees.

49% of respondents from financial services companies have registered an increase in the technical sophistication of attacks on their customers.

63% of respondents classify infected websites as an attack vector most likely to lead to a compromise of their customers' online security.

And the cyber-criminals are getting smarter...

From the frontlines...

What worries you most about attack trends in terms of the threats with the greatest potential to impact your organisation financially?

From business

- Number of attack vectors, amount of intelligence to digest, insufficient headcount to cope with all angles.
- That the attackers may have access to more resources than we could deploy to defend against them.
- Attacks are becoming more subtle and are harder to spot and counter.
- Ever increasing sophistication, making them harder to detect/taking longer to do so, thereby potentially creating more damage before they are discovered and rooted out.
- Difficulty of identifying and countering a specifically targeted attack.
- Inability to institute protective countermeasures.
- End users in organisation not prepared enough to identify risks.
- Complacency of the users and their general lack of security awareness.

From government

- The rising level and sophistication of attacks will place an unsustainable burden on our information assurance budget.
- The trend to launch multiple attacks at the same time but at different targets within the organisation.
- Use of our data to commit fraud.
- Lack of buy-in at the executive level.
- The targeted nature of the attacks identifying key staff who have poor IT security knowledge and are also time poor so they open [emails] without checking.

From the vendors

- Attacks can be expected on many channels and it is difficult to come up with a generic and cost-effective solution.
- Customer data is becoming harder to protect due to the disconnect between the business and security functions.
- Concentration of multi-attacks causing major break to IT systems.
- That business owners or risk owners like to assume or calculate in their minds that the risks of electronic attacks to their company is really low and so take no measure to even monitor if they're currently being attacked.
- Attacks bringing down our website.

From the editor

**Jonathan Hawes,
Editorial Director of the
e-Crime Survey 2009**

The economic crisis has served to elevate the profile of certain risks linked directly and indirectly to information and IT security, one of which is that of data quite literally marching out of the door. In recent months a succession of stories have reported that corporate information is under threat from employees who may steal data for personal profit, revenge, or as a potential leveraging tool for obtaining new positions elsewhere.

Whether you relegate such bad-tidings to the realm of vendor-hype, or believe such reports to accurately depict the status quo, one thing is certain: The issue, while in vogue, is not breaking news for security practitioners.

A more challenging area to address, and one that is equally critical in the current climate from a strategic standpoint, is whether security-focused departments will find themselves able to develop proactive models of business defence that effectively protect organisations and their customers from the accelerating phenomenon of e-Crime.

The majority of survey respondents identify budget as the primary bottleneck to delivering a proactive level of service. In an environment characterised by the exponential multiplication of economic and commercial risk the implications of this are far from encouraging.

This survey indicates that the level of technical sophistication in criminal endeavours to compromise enterprise networks and online customers is rising; the majority of respondents believe the increase in unemployed IT security professionals during the recession will swell the ranks of the cyber-criminal underground economy; fraud attacks on customers are more sophisticated and more targeted.

Time will tell whether security spending weathers the economic storm. Considering the threat matrix, it can only be hoped this will be the case. Unfortunately, if the recent history of the financial markets has shown us anything, it is that the business of optimistic projections is a risky one.

As massive drops in profit are reported on a daily basis, areas of operation that promise to deliver fast money will have a magnetic attraction. From a client-facing perspective, most legitimate organisations with any commercial savvy will look to the Internet as a way of maximising revenue. For those already established within the online environment, the preoccupation will be how to find new and innovative ways to increase their returns.

At the same time those with fewer scruples and a knowledge of the rich pickings available will turn to cyber-crime, inevitably leading to further advancement, syndication, and expansion of malicious activity across the online and electronic landscape.

The clear message from this survey to executive boards and budget holders is that departments with responsibility for e-Crime must continue to be provided with sufficient resources in order to protect assets, defend against attack, and facilitate – as far as is possible – a low-risk environment for ongoing commercial growth.

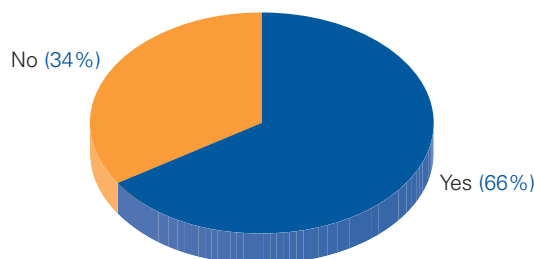
Both AKJ Associates and KPMG extend their sincere thanks to all those who participated in the survey this year. We hope that you find the report that follows both interesting and informative.

Key findings: On the recession

- 66% of respondents agree that an increase in out-of-work IT professionals during the recession will lead to more people with technical skills joining the cyber-criminal underground economy.

Do you think an increase in out-of-work IT professionals during the recession will lead to more people with technical skills joining the cyber-criminal underground economy?

All respondents

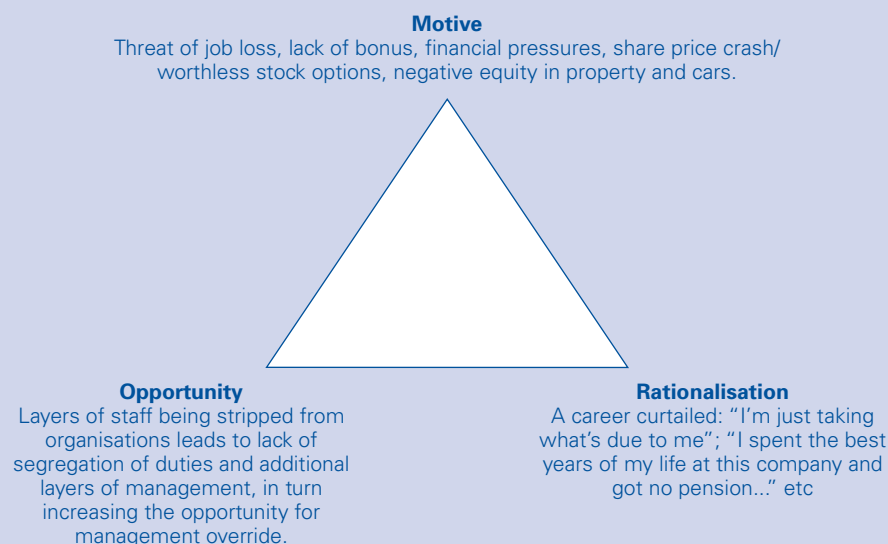


An influx of technically proficient individuals with security backgrounds into the cyber-criminal underground economy seriously raises the stakes in the electronic arms race, shifting the odds of success in favour of those who develop crime-ware.

As the recession has deepened, finances are tightening across corporate functions. Several studies last year indicated security budget holders felt they were likely to survive unscathed. Whether such optimism remains is questionable.

Motive, opportunity and rationalisation for fraud can coincide during an economic downturn.

The fraud triangle



In 2008 fraud perpetrated by managers, employees and customers trebled compared to the figure of 2007. These figures tend to indicate that the threat of fraud during the recession will only increase and we have yet to feel the full impact of the credit crunch.



From the frontlines...

What worries you most about attack trends in terms of the threats with the greatest potential to impact your organisation financially?

- The increasing sophistication arising from unemployment amongst experts in this field.
- Software and hardware developers prepared to provide services to anyone/anywhere for the right price.

As companies implement measures to cut spending it is increasingly likely that “workflow reorganisation” will lead to some business functions being combined or outsourced. The impact of structural changes will inevitably lead to some increase in out-of-work IT professionals, whether due to contractors being laid off, departments being forced to make cuts, or companies going bust.

At the same time, students or experienced professionals entering the IT job-market are likely to discover that job opportunities are, to coin a financial oxymoron, in a phase of negative growth.

- **In the current economic climate, the internal e-Crime risks selected as being of most concern by the highest number of respondents are: “Theft of customer or employee data by insiders or ex-employees” and “Knowledge of weak points in business processes/systems being deliberately exploited by insiders or ex-employees”.**

What internal e-Crime risks are of most concern in the current economic climate?†

All respondents

Theft of customer or employee data by insiders or ex-employees	64%
Knowledge of weak points in business processes/systems being deliberately exploited by insiders or ex-employees	62%
Theft of intellectual property or business sensitive data by insiders or ex-employees	61%
Loss of undocumented business knowledge (e.g. processes, encryption keys) relevant to security	38%
Employees placing personal information on the Internet that can be exploited by attackers	36%
Knowledge of weak points in business processes/systems being sold	27%
Other	3%

Respondents from IT security

Theft of customer or employee data by insiders or ex-employees	64%
Knowledge of weak points in business processes/systems being deliberately exploited by insiders or ex-employees	60%
Theft of intellectual property or business sensitive data by insiders or ex-employees	58%
Loss of undocumented business knowledge (e.g. processes, encryption keys) relevant to security	46%
Employees placing personal information on the Internet that can be exploited by attackers	39%
Knowledge of weak points in business processes/systems being sold	21%
Other	4%

† Percentages shown indicate a proportion of total responses.

From the frontlines...

What worries you most about attack trends in terms of the threats with the greatest potential to impact your organisation financially?

- The increase in the number of skilled IT professionals in the industry who have left the organisation and with intimate knowledge of the organisation and its internal functions, people and processes.
- The potential for those who are disgruntled and out of work, and have up to date system and process knowledge becoming involved in malware design.

Customer or employee data would offer a lucrative and tempting source of revenue, whether sold to competitors or cyber-criminals. A working knowledge of vulnerabilities in processes and business systems that are open to exploitation could provide current or former employees with a means of severely disrupting operations.

The abuse of privileged information would also create the greatest scope for financial loss from internal fraud or externally generated, financially motivated malicious attacks.

The sale of information relating to weaknesses in applications hosted on the web should be a particular concern. Just under half of the total respondents (48%) selected this option as one of the top three areas of most concern when answering the question "What areas of IT infrastructure concern you most in terms of vulnerabilities that can be exploited by cyber criminals?"

Tracking and mitigating insider security risks in a recession

IT professionals are often the people in the organisation who have "super-user" access, with knowledge of the strengths and weaknesses of the company's IT security. This knowledge would be extremely valuable to the cyber-criminal underground community.

The key to limiting the risk of this occurring can be summed up in two words: "Monitoring" and "Deprovisioning." However, internal system monitoring and auditing is commonly overlooked, which is often linked to the implicit trust of existing employees.

Organisations typically investigate system logs and user activity only when any concerns have been highlighted within the organisation. This therefore leaves a big window of opportunity for the more cautious and nefarious insider. Without a structured process around user activity monitoring, organisations are often left clueless with regards to insider threat levels.

For leavers of the organisation, it is paramount that they are properly deprovisioned of all IT devices and systems, and that all of their accounts and privileges are properly revoked from systems and networks. Those organisations that do not have a dedicated and comprehensive process around deprovisioning of leavers will expose themselves to potential security breaches by those ex-employees. In essence, a robust Identity Management implementation is required to mitigate the risks in this area.

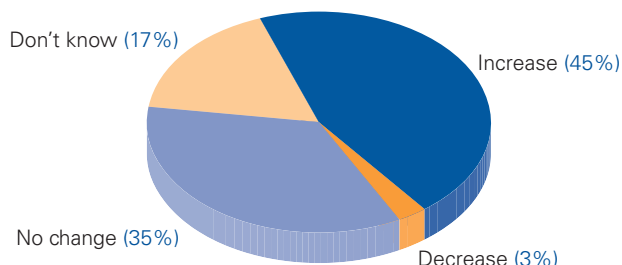


Key findings: On fraud

- 45% of all respondents have seen an increase in fraudulent activity reported by customers.

Trends in fraudulent activity reported by customers

All respondents



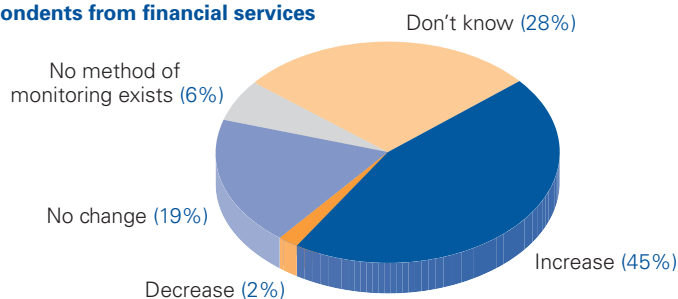
The online consumer's computer represents the point most susceptible to compromise in relation to online transactions and interactions between commercial enterprises and Internet clients.

E-crime is driven by financial motive. Because the online consumer represents a soft-target when compared with corporate networks and web gateways it is logical that cyber-fraudsters will continue to focus their attention on those who use e-commerce services.

- 45% of respondents from financial services registered an increase in volume of attacks on their customers.

Trends in volume of attacks on customers

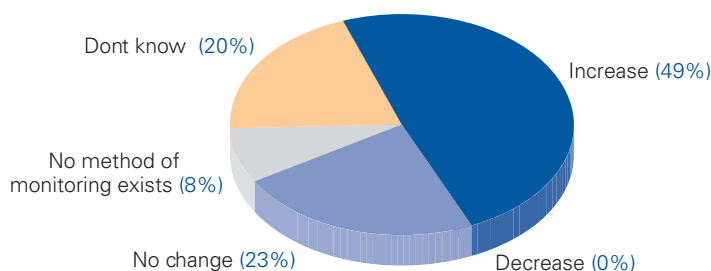
Respondents from financial services



- 49% of respondents from financial services companies have registered an increase in the technical sophistication of attacks on their customers.

Trends in technical sophistication of attacks on customers

Respondents from financial services



From the frontlines...

What worries you most about the future of malware attacks?

- Increasing sophistication due to funding from organised criminals. Security professionals are continuing to be behind them in terms of progress. Personal/sensitive data is seen as a valuable currency and more concerted effort is put behind developing malware to harvest this information.

In the case of financial services, as the volume of attacks on the consumer has risen, so has the sophistication and targeted nature of attacks. This result would seem to confirm that malware designed to target interactions between financial institutions and their customers is at the cutting-edge.

Commentary by:

Uri Rivner, Head of New Technologies – Identity Protection and Verification Solutions, RSA, The Security Division of EMC

The past year has seen a dramatic increase in Trojan operations as infection and anti-virus evasion technologies improved. Organised cyber crime groups have stepped up their activities: for instance, the rate of infection in the Sinowal Trojan intercepted by RSA FraudAction Labs jumped from 3000 new PCs infected during March 2008 to almost 30,000 new devices infected during September 2008.

Trojan kits such as Zeus and Limbo are now so affordable and user-friendly that many non-sophisticated fraudsters that were previously focused on Phishing are now diversifying to crimeware. If your Trojan isn't configured for a specific target bank, worry not: for \$10 you can buy a custom HTML injection template for use with your Trojan. It will address any specific defences used by the bank, and even automatically check the balance for you. And for less than \$300 per month you can even buy a "Software as a service" subscription to a Zeus Trojan hosted in a "bulletproof" server and connected to an infection kit. Just pay the subscription, sit back, and start infecting machines around the world and harvesting the victim's credentials.

Two-factor authentication such as one-time passwords and transaction signing triggered a rapid arms race with the Trojan manufacturers, primarily in Europe and Latin America. Using a combination of session hijacking and social engineering techniques, Trojans are capable of bypassing even the most robust visible defences. This made many financial institutions look for additional, invisible lines of defence such as device profiling, transaction monitoring and Trojan counter-measure services, as well as out-of-band phone based authentication.

The scaled-up technical infrastructure means more credentials are being harvested than ever, but emptying the victim's accounts requires a similar scale-up of the operational infrastructure. Luckily for the cash-out operators, the difficult financial times increase the number of people answering "work from home, earn a lot of money" ads that are in fact mule recruitment scams. In a particular scam exposed by RSA, the fraudsters got 1,925 "applications" and eventually "hired" 33 mules.

Finally, the threat of Trojans now extend beyond financial institutions. Thousand of corporate laptops are carrying a Trojan after the employee got infected like any other consumer at home, and then brought the device with him to the office, connecting it to the corporate network. Fraudsters haven't figured out an effective way to capitalise on this unexpected pot of gold, but it's only a matter of time before they do...

From the frontlines...

What worries you most about the future of malware attacks?

- The increasing intelligence of automated attacks and shortening response windows.

Spotlight on fraud malware and artificial intelligence

The rise of the Trojans

If you were a cyber-criminal, the perfect Trojan would constitute something that couldn't be seen and couldn't be wiped. You'd be able to interact with it, but you could also leave it to go about its business automatically. It would have multiple functionalities, modes, and information capture protocols. And if it got discovered, it would be able to erase itself completely so that it couldn't be analysed. The bad news is that the coders on the dark-side are 90% there.

- **This tape will self-destruct in 5 seconds...**

Targeted malware has, for some time, been designed to circumvent detection by security suites based on company specific profiling. But now, once security suites have been bypassed, Trojans can "sense" if they have been detected and wipe themselves completely from the operating system before they can be captured. This effectively covers their tracks, makes reverse engineering impossible, and hinders efforts to find out what vulnerabilities were exploited.

- **Your computer has been successfully updated...**

Once successfully installed, the new breed of malware has a continuing dialogue with its command and control centre. When a new version of code is available, perhaps offering greater functionality or better shielding from detection, updates can be applied.

- **I want to break free...**

If malware detects it is being hosted in a virtual environment, it may erase itself and all traces of its existence or try to extract itself in order to get a foothold on the operating system that controls the environment. Where a number of companies are hosted on the same server, breaking through the virtual boundary allows for opportunistic malicious activity.

- **Ghosts in the machine...**

Tigger.a

- 1) Install yourself on a computer and then bury yourself in the master boot record.
- 2) Hide in a part of memory that is concealed from the operating system.
- 3) Uninstall all Adobe products to decrease the opportunity for other malware to infect your host.
- 4) Wait for a fraudster to connect remotely to the computer; then provide a shadow desktop and keep all activity hidden from the user.
- 5) With your powerful scripting engine, receive and act on instructions.
- 6) Capture everything that is typed when the user accesses specific websites.
- 7) If security software tries to access or profile you, give no information back.
- 8) When nothing else works and the user reformats the drive, don't worry. Because you reside in memory, you'll be there when they boot up.

Key findings: On fraud

DDoS is dead, long live DDoS!

The fact that 33% of financial services companies have seen an increase in illegitimate login attempts to customer accounts highlights a growing possibility of both Denial of Service (DoS) and unauthorised access attempts against survey respondents. If online applications implement an account lockout threshold for a predefined number of unauthorised login attempts, then the account is typically locked or deactivated for some period of time.

This property can be exploited by attackers through the use of automated attacks that attempt invalid login attempts against a list of valid usernames. The result of such activity is each account becoming locked, thereby invoking a DDoS against the "victim customers"; and increasing the load on any backend helpdesk facilities.

The bigger concern in this area lies with those applications that do not implement an account lockout facility. This allows an attacker possessing a list of valid usernames to attempt a brute force dictionary attack that may eventually result in unauthorised access.

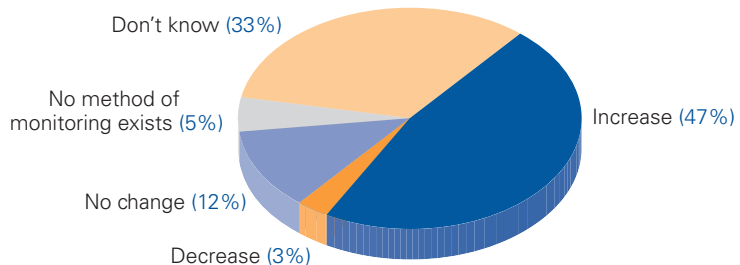
This statistic identifies the need therefore for respondents to evaluate their customer-facing authentication mechanisms and the associated procedures around handling invalid access attempts. This is necessary from both a security and business continuity perspective.



- **47% of respondents from financial services have registered an increase in volume of specifically targeted attacks on customers.**

Trends in specifically targeted e-Crime attacks on customers

Respondents from financial services



Sophisticated phishing that abuses human insecurities, or the trusted relationship between customers and businesses, continues to trick users into providing personal and sensitive information. PCs infected with malware that include key-logger functions, for example, allow fraudsters to remotely harvest data. But this is only one half of the story.

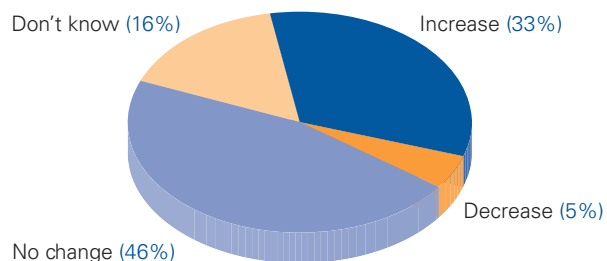
Citizens of the brave new electronic age have an ever-increasing digital footprint. The proliferation of social networking as a preferred media of communication provides a rich information repository for cyber-fraudsters to draw on. Meanwhile, the centralisation of public records on national e-government databases can only serve to increase the attack surface.

Because of the spectrum of granular information that can be easily acquired on Internet users, socially engineered attacks on institutions and individuals will only grow in their authenticity.

- **33% of financial services companies who responded to the survey have seen an increase in illegitimate login attempts to customer accounts.**

Trends in illegitimate login attempts to customer accounts

Respondents from financial services



A range of available technologies exists to detect fraudulent activity. With attempts to compromise account security on the rise, the results of the survey indicate that budget spent on data that can help prevent illegitimate logins is by no means wasted. However, there are implications for companies experiencing a high volume of fraudulent login attempts beyond that of account takeovers.

Commentary by:

Daniel Chapman, Forensic Investigations Manager, TNT Express

- **When asked about trends in illegitimate websites exploiting intellectual property, such as brand or logo, 29% of respondents to the e-Crime Survey said that the problem was increasing, 44% indicated “no change”, and 4% indicated a decrease.**

A recent Japanese study shows a 15.5% year-on-year annual growth in online crime, and whilst there are no directly equivalent Western figures, this survey and the experiences of TNT appear to strongly support these results.

Despite this general growth, 4% of respondents showed a reduction in the problem of illegitimate websites that abuse intellectual property but it's far too early to begin celebrating any kind of victory.

The problem when trying to assess the level of IP theft and abuse online is that evidence can be very hard to find unless it is reported by the victims of the frauds, and they don't always feel comfortable stepping forwards. Many companies simply do not have processes in place to respond appropriately to these individual reports and it can be extremely tempting to react defensively rather than welcoming the report and supporting the individual. A defensive response runs the risk of actively discouraging reports whilst failing to address the root cause, producing a false impression of falling incidents.

To add further complexity, the true measure of the damage done to our reputation by fraudulent sites may not be how *many of them* there are, but how many victims each site produces. Is more damage to reputation done from 50 sites that have a single victim each or one site with 100 victims?

- **6% of respondents from financial services indicated a decrease in the volume of illegitimate websites exploiting intellectual property, 47% indicated no change.**

The people with the most experience of large-scale online impersonation are the financial sector, and that may explain the slightly higher percentage of financial institutions reporting “no change” – they are at least “holding the line”. This is a positive achievement for the sector but the theory of crime displacement suggests that as financial institutions become increasingly “hard targets” the criminals will shift towards easier corporate victims. These new victims are likely to be drawn from product and service providers previously untouched by online IP exploitation.

- **23% of the total number of respondents selected “Don't know” when asked about trends in illegitimate websites exploiting intellectual property.**

Considering this possible change of criminal strategy it is concerning that just over a fifth of all respondents state that they “Don't know” the scale of the problem affecting their company. For these companies investment in processes that will measure the threat is increasingly important in order to avoid becoming “soft targets” for the criminals. Those of us who already have measurement tools in place need to invest further in order to reassure ourselves they are working correctly and producing pragmatic risk values.

Given the current economic climate any investment will be hard fought and must be well spent, but as this is exactly the type of climate in which frauds are likely to increase we need to be ready to react. The threat matrix is complicated and depends on the markets we operate in, what form of IP theft is occurring, and the amount of publicity incidents receive.

What cannot go un-addressed however is the need to assess all of these factors and implement controls suitable for your unique situation.

Spotlight on phishing

Think phishing is no longer a threat to your customers? Think again....

■ **MarkMonitor's Brandjacking Index of March 09 identified that financial services is still the primary target of phishing style attacks and saw a 51% rise during the second half of 2008, as fraudsters attempted to profit from the flux and confusion in the sector with many individuals moving their savings more actively.**

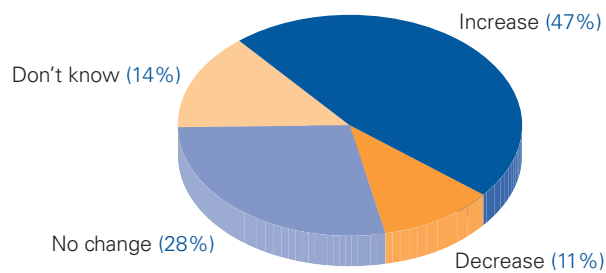
■ **Sectors outside of payment/auction services, financial and retail saw a 135% growth in phish attacks during 2008, according to MarkMonitor's March 2009 Brandjacking Index. This group includes gaming, betting and recruitment sites which have seen a significant growth in usage on the Internet.**

■ **There continues to be a trend to widen the net of phishing with 444 new organisations "impersonated" in phishing attacks during 2008, as identified by MarkMonitor's March Brandjacking Index.**

■ **The United States continues to host the highest percentage of phish sites (36% during 2008) which can be explained by it having such a large concentration of the World's hardware and ISPs. The Russian Federation and the Republic of Korea were the only two other countries that were amongst the top five hosting phish each quarter of 2008.**

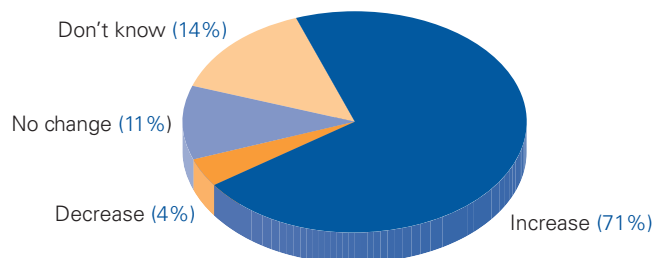
Trends in volume of phishing attacks targeting customers

Respondents from financial services



Trends in specifically targeted nature of attacks on customers

Respondents from fraud investigations



From the frontlines...

What worries you most about attack trends in terms of the threats with the greatest potential to impact your organisation financially?

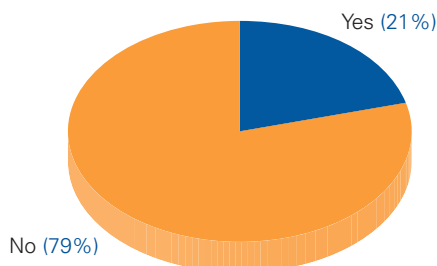
- Phishing is a significant vulnerability for my organisation. We are increasing customer awareness but have observed a trend in increased losses due to customer inexperience.

Key findings: Online consumer security

- 79% of survey respondents do not believe that security software based on signature detection offers a sufficient level of protection to Internet users.

Do you believe that security software based on signature detection delivers a sufficient level of protection to Internet users when you consider the variants of malware threats to those users?

All respondents



As the recession bites into consumer spending, the percentage of renewals for paid licences of security software could fall dramatically. However, whether the luxury of security is something home users decide they can't afford, the majority of survey respondents do not believe that signature based detection offers Internet users sufficient protection.

Security software used to be seen as the first line of defence in keeping computers that connect to the web free of infection. However, solutions that use signature detection to protect computers from malware are only as up-to-date as the information gathered by vendors and applied to machines in updates. By its very nature this method of protection is reactive.

From the frontlines

What worries you most about the future of malware attacks?

- Malware is becoming a more and more pernicious attack vector against consumers. At this point, anti-virus products are more or less worthless as protection mechanisms. A new breed of anti-virus products needs to emerge which can really address the problem effectively.
- That vendors will continue to use a failing technology and that companies will fail to grasp the part that true security education has to play in all of this.
- Keystroke loggers and screen capturing have reduced the effectiveness of passwords, even two factor authentication can be compromised by a man in the middle attack. Without a secure method of authentication customers will have no confidence in the technology and refuse to use it.

Commentary by:

Ian Amit, Director of Security Research, Aladdin Knowledge Systems

Focusing on the survey statistics concerning attack vectors and signature detection, and cross-referencing our research material from the past 6–8 months, the prevalence of the web-attack vector proves it is not just a fad but a successful business. Firewalls and other network protection systems are rendered practically blind the second that users are allowed to access the web (via port 80 and 443).

Essentially, traditional security measures are not keeping up with MalWeb – and the survey reflects that pretty accurately. When you count in the increase in sophistication of attacks from the technical side as well as the “human” factor, (enticing users to perform actions that help the attack succeed), detection becomes much more than a “sign-and-update” task. It’s more like a complex reconnaissance and intelligence mission – it’s about spotting malicious components in legitimate websites, coping with behavioural aspects of code and user, and still – like any security solution – providing a high level of usability.

Last but not least, we are seeing – and the survey confirms that – an increase in targeted attacks on the more profitable industries. Finance and healthcare are marked as a premium when looking at the e-Crime business MO (Modus Operandi).

In view of the high volume of sophisticated crimeware designed specifically to hijack home computers, it appears that confidence in the ability of security suites to keep up with the cyber-criminals is low.

Heuristic detection methods offer no real alternative solution considering the volume of ways that criminals can tap into computers. Furthermore, because security software and malware both operate on the same part of memory, if malware can effectively shut down the software, the solution is still rendered impotent.

- **Poisoned websites, infected email, phishing, and social networking sites are the vectors seen as most likely to compromise customers' online security.**

Which attack vectors do you think are most likely to lead to a compromise of your customers' online security?[†]

All respondents

Infected websites	63%
Infected email	48%
Phishing	48%
Social networking sites	43%
Popup warnings and download prompts	25%
Physical hacks	22%
Instant messenger	13%
Other*	10%

[†] Percentages shown indicate a proportion of total responses.

* Of respondents who selected "Other," vectors highlighted were file sharing, peer-to-peer applications and infected USB drives.

The challenge of how to secure customer systems and make the Internet a safe place to do business is one that will only grow in complexity. Looking at the list of vectors rated as "most likely to compromise customer security" it is little wonder that the topic of whether or not the Internet in its current form will continue to be a viable portal for e-commerce is moving beyond the realms of academic debate.

- **Online consumers, followed by government, are viewed as contributing the least to the battle against e-Crime.**

The Internet is, inescapably, the future of revenue generation. However, the relative anonymity that characterises interactions between corporate networks and online customers, as well as the manner in which transactions are conducted, creates huge opportunity for abuse.

Online consumers stand directly in a line of fire that is getting more hazardous as time progresses. Yet, regardless of the mounting threat to this demographic, the perception of survey respondents is that this is exactly the group that is doing the least to contribute to the fight against e-Crime.

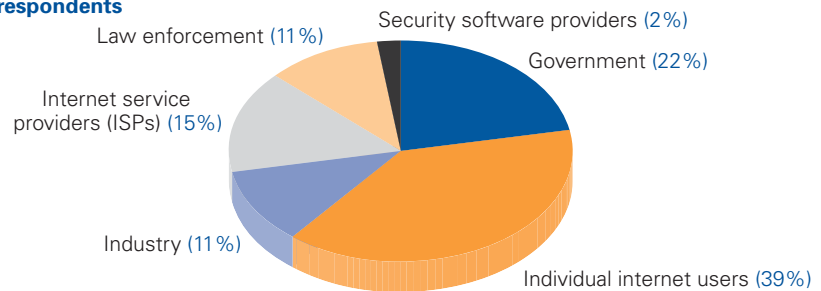
From the frontlines...

What worries you most about attack trends in terms of the threats with the greatest potential to impact your organisation financially?

- Users do not seem to be learning from media coverage and appear to be no less susceptible to attacks. Education is key but users do not appear to be interested in learning.
- That large numbers of consumers will lose their trust in the safety of the Internet.
- Capability to get user/customer education that is effective to them in a timely manner.

Which group do you think is currently the least active in combating e-Crime that targets e-commerce operations and online banking services?

All respondents



Commentary by:

James R Gay, Chief Information Security Officer, Travelex

This is an interesting response, and I think the answer may have been influenced by the question in many cases. It does seem that there is a ground swell in holding Government accountable for some portion of blame in the rise in e-crime. There is also an argument that once again we (IT) blame the users for the failures in our systems, we should perhaps ask; "Are we supporting the users with the right tools?" rather than "Are they active in the fight against what arguably many just don't understand?"

- **An increasing volume of attacks against customers was registered by 39% of respondents. Only 1% indicated a decrease.**

- **According to 40% of total respondents there has been an increase in the technical sophistication of attacks against customers.**

Deciding how to educate users about threat and promote a collective security consciousness is not without its problems. Software and browsers must tread a thin line between usability and security; using an alert method such as pop-up warnings runs the risk of them appearing so regularly that users may simply disregard them; providing indications of whether sites are secure relies on users actively checking URLs and certificates.

When one considers that advice such as "make sure anti-virus is installed and up to date" is no guarantee at all of protection, the question of how to implement a meaningful baseline for consumer safety online is an exceptionally tricky one. For the time being, the matter of how best to engage consumers remains an unknown quantity.

Key findings: On e-Crime and enterprise defence

Statistical analysis

Only 1% of respondents have seen a decrease in the technical sophistication of attacks on their network. While 33% registered no changes, 41% registered an increase.

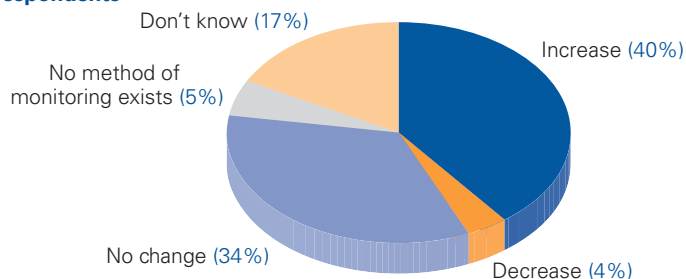
The results above are curious. Respondents registering no change or a decrease in the sophistication of attacks on their networks imply they have a current benchmark of attack sophistication. Such a benchmark cannot realistically exist, as attack sophistication could be far beyond one's own interpretation of the current state of play. The applicable cliché in this area is: "If you don't know what you're looking for, how do you know when you've found it?" This means that 38% of respondents may therefore be more vulnerable to sophisticated attacks against their infrastructure than they believe.



Attack trends: the network

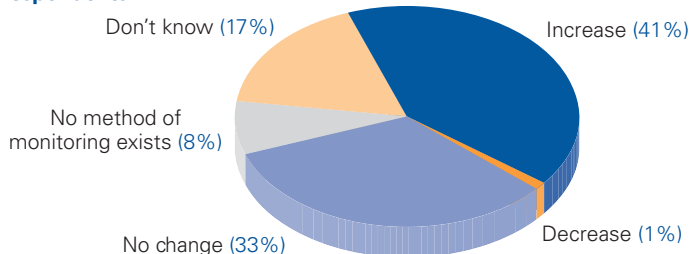
Volume of attacks

All respondents

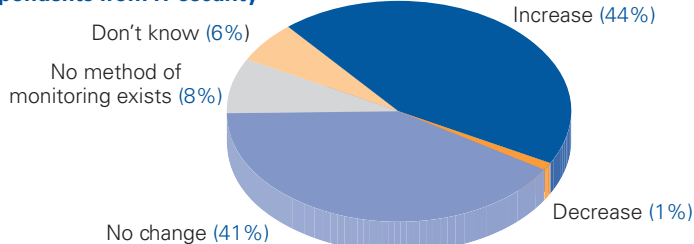


Technical sophistication of attacks

All respondents

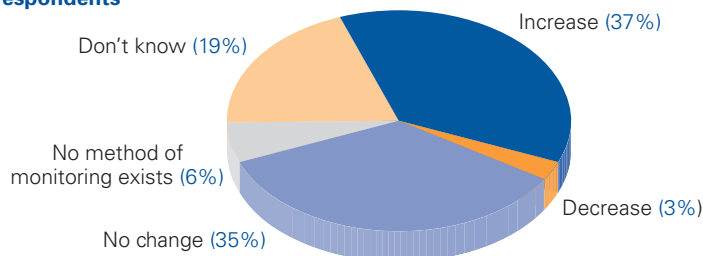


Respondents from IT security

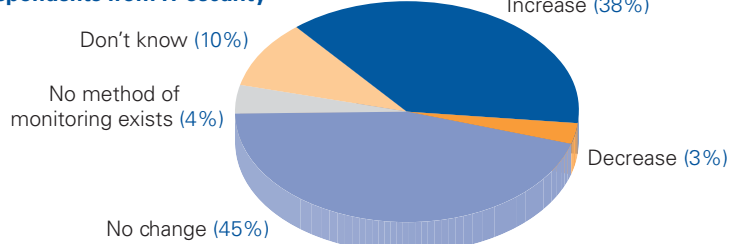


Specifically targeted e-Crime attacks

All respondents



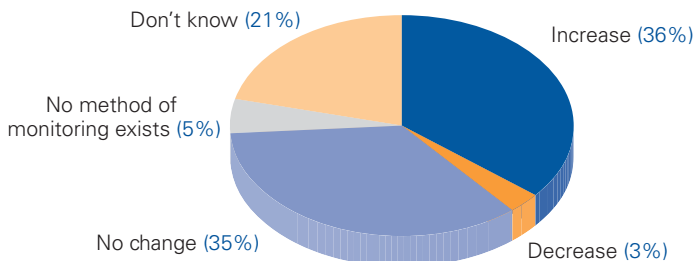
Respondents from IT security



Attack trends: the web gateway

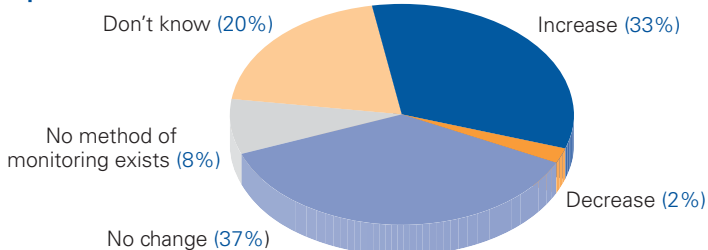
Volume of attacks

All respondents

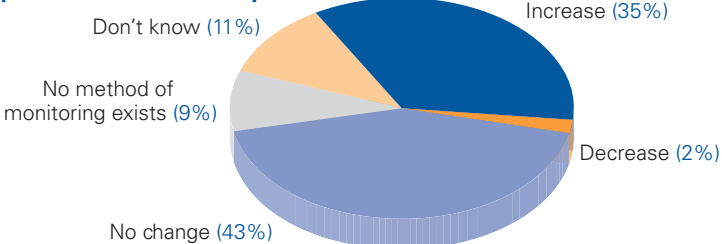


Technical sophistication of attacks

All respondents

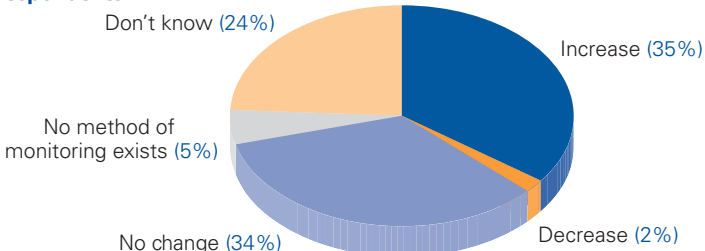


Respondents from IT security

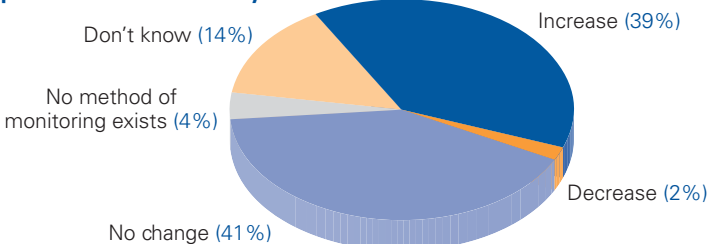


Specifically targeted e-Crime attacks

All respondents



Respondents from IT security



From the frontlines...

What worries you most about attack trends in terms of the threats with the greatest potential to impact your organisation financially?

- Attacks or data compromise which occurs at 3rd party vendors. We do not know the extent a 3rd party maintains and monitors security controls so our vision is limited – and assumed risk is increasing.

e-Crime defence

Winners PODIUM by all respondents

Which business assets would you currently classify as high-risk targets from e-Crime attacks targeting your network?†

1st	Customer data	76%
2nd	Personal identifiable information of customers	60%
3rd	Login/password information and account information	53%
and in last place*	Business sensitive information e.g. P and L figures	

† Percentages shown indicate a proportion of total responses.

* Classified by the lowest percentage of respondents as being at risk

Winners PODIUM by all respondents

Which external threats are you currently most worried about in terms of your ability to defend against them and their impact on your organisation?†

1st	Attack on the network aiming to compromise customer data or business sensitive data	73%
2nd	Compromise of computers used by Internet users who interface with your web gateway	64%
3rd	Breach or compromise of business partner/service supplier (that stores or has access to your customer data or business sensitive data)	57%
and in last place*	Attack reducing the availability of the web gateway	

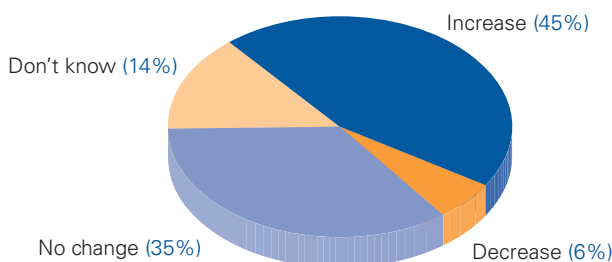
† Percentages shown indicate a proportion of total responses.

* Classified by the lowest percentage of respondents as being a concern.

One to watch

Trends in the volume of phishing targeting employees

All respondents



From the frontlines...

What worries you most about the future of malware attacks?

- Their growing volume and the low quality code/lack of high quality penetration tests by web application software suppliers.
- Becoming more and more targeted and less detectable both by measures and end-users.

Internal attack vectors

Most high profile data loss cases seem to be those of lost computers and mobile devices. The results from the survey reflect this and it remains a key concern for companies and an area of control weakness without security policies in place around personal use of mobile devices and appropriate encryption. Email remains a major cause of concern, particularly web-based email – providing the opportunity for misuse by employees to steal company data.

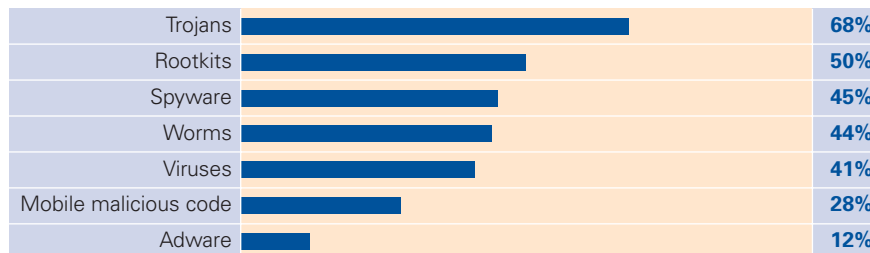


Protecting the infrastructure

- Trojans are the payload that concerns the majority of security professionals in terms of business impact on the network.

Which payloads are of most concern in terms of business impact regarding your network?†

All respondents

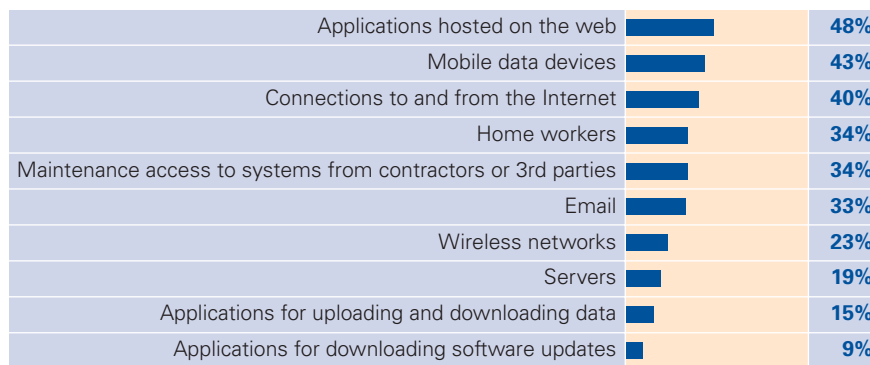


† Percentages shown indicate a proportion of total responses.

- Applications hosted on the web account for the greatest concern in terms of IT infrastructure vulnerabilities that can be exploited by cyber-criminals.

Which areas of your IT infrastructure are of most concern in terms of the vulnerabilities that can be exploited by cyber-criminals?†

All respondents



† Percentages shown indicate a proportion of total responses.

Commentary by:



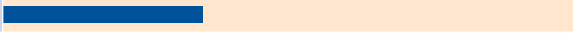

James Gay, Chief Information Security Officer, Travelex

Interestingly where traditionally security has defined the highest risk as people having access to the bowels of systems, the plethora of bugs, errors and code exploits as well as the absolute mass of people on the net has shifted focus to outward facing systems. Social engineering and blended attacks may however cause us to look again at our internal protections in the future, but for now it is obvious our trust levels in Internet applications is not high.

- **Poisoned websites and downloads are the attack vectors targeting IT infrastructure which concern the most respondents in terms of the difficulty in defending against them.**

Which attack vectors targeting your IT infrastructure concern you most in terms of the difficulty in defending against them?†

Respondents from IT security – top 4 results

Poisoned websites		50%
Downloads		39%
Email attachments		35%
Spoof websites		33%

† Percentages shown indicate a proportion of total responses.

Spotlight on the wild wild web

Today’s website compromises are no longer the defacements of yesteryear. Unlike in the past, these compromises are engineered to be as non-noticeable as possible. The intent is no longer a prank; the intent is to foist malware onto the computers of those visiting the sites. The majority of that malware is designed for data harvesting.

Attackers are employing multiple exploits targeting a wide array of installed software. Successful exploit enables the silent delivery of malware onto the system. Unlike the drive-by downloads in the early part of the new millennium which were highly visible and often left users wrestling for control of their system, the modern day drive-by download is specifically designed to be as unobtrusive as possible.

Automated attacks throughout 2008 have led to immeasurable numbers of website compromises. To put this number into perspective, during a single outbreak of one wave of SQL injection attacks, ScanSafe STAT tracked the impact on 5 industry verticals (government, travel, medical, finance, and travel) and recorded 780,000 compromised Web pages resulting from just that one single attack and from just those specific verticals.

ScanSafe STAT analysis reveals a high degree of targeting involved with today’s Web malware. The malware delivered to victims’ computers is largely dependent on the company, industry, and country with which that victim is affiliated. As the level of sophistication and targeting increased throughout 2008, ScanSafe STAT also observed correlating increases in malware that employs ARP poisoning and other man-in-the-middle attacks. Thus not only are backdoors and data harvesting trojans installed on the system, but attackers are also able to intercept network and Internet traffic within that segment of the network.

In summary, today’s malware is a massive data harvesting operation and compromised websites are being used as the predominant delivery mechanism for that malware. Once on the system, the malware is highly configurable, enabling attackers to remotely control its behavior – including the ability to specify what data is to be harvested by the Trojans and how that harvesting should occur.

Mary Landesman, Senior Security Researcher, ScanSafe

From the frontlines...

What worries you most about the future of malware attacks?

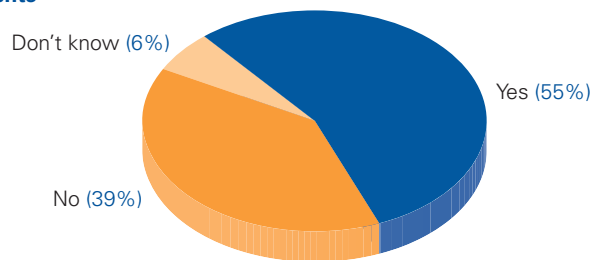
- That they become more complicated and that they’re able to bypass the security placed on the perimeter especially for users who unknowingly accessed a site that has the malware.
- The company manufacturing the software and hardware is the same one doing the malware attacks.

Malware

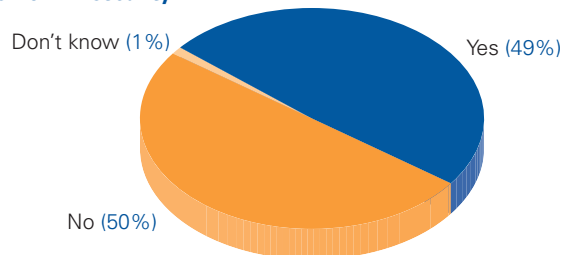
- Just over half of respondents believe their organisation is sufficiently protected against malware.
- Some security functions are more confident than others, but 50% of respondents from IT security are not optimistic.

Do you believe your organisation is sufficiently protected against malware when considering internal Internet usage trends, attack vectors, potential targets, security update procedures, and the risks associated with compromise to your business?

All respondents



Respondents from IT security



While anti-virus and malware protection software can go some way in reducing the associated risk levels with email attachments and poisoned websites, they do not constitute a solution, and are only effective when coupled with user awareness and education on the risks in this domain. It is not sufficient for users to be simply told that clicking on links or downloading attachments is “not good”. Without demonstration and explanation of the issues around these activities users cannot truly appreciate the issues and exercise appropriate caution accordingly.

Similarly, the use of anti-virus and malware protection software can often increase the “riskiness” of user behaviour when emailing or web browsing. This is akin to theories that when motorists wear seatbelts they may be more inclined to drive faster – users with antivirus or malware protection may therefore be more likely to download suspicious-looking emails, believing that any risk will be mitigated by the anti-virus software. This is not an acceptable attitude given that anti-virus signature updating is an ongoing “catch-up” process, and that vulnerabilities exist in anti-virus software packages, as identified in various independent research studies.



From the frontlines...

What worries you most about the future of malware attacks?

They are constantly evolving and lack of budget & resources to keep up effectively.

The current exploit times show a closing detection and respond window which means a “big” one is always just round the corner.

Their flexibility and adaptability ensure they evolve with each version and vector.

The possibility of deep-rooted malware infection that remains undetectable by anti-malware products. The chipset as the next battleground.

The increasing intelligence of automated attacks and shortening response windows.

We have already had an attack where the infection was dormant, remaining undetected, for 10 months. How many more of these are already on our computers?

The emergence of multi vectored malware which uses a combination of technical and social techniques to propagate, hide and scavenge and disseminate sensitive business information.

Our poor level of workstation security, due to our application suppliers who, even though pressured, do not make their software to support newest browsers, acrobat readers, etc.

That we continue to tackle a global, borderless problem on a national basis.

Ineffectiveness of most commercially available controls systems (without wrecking the business functionality of o/s & office support tools).

We’ve seen malware recently that specifically targets us!!

That the move to “deperimeterisation” of corporate networks will be overtaken by attacks on home/remote users and malware will impact the business via these vectors.

The quality and accuracy of the heuristic detection mechanisms.

The potential for such attacks to become virtually undetectable and exceedingly difficult to remove.

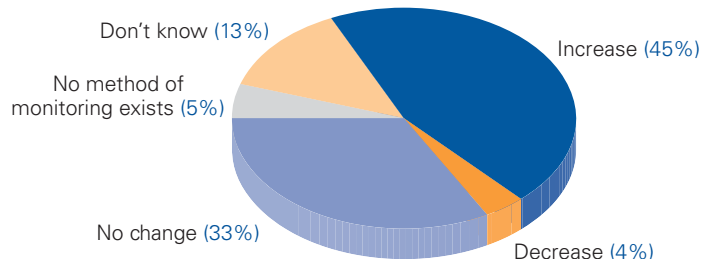
That viruses will encompass cryptography technology in their reproduction (cryptovirology) therefore rendering antivirus applications that perform signature matching pretty much useless in defence. I’ve yet to see an antivirus product capable of managing cryptoviruses, though I have seen real-life cryptoviruses already causing damage on corporate networks.

Key findings: On cyber defence and critical national infrastructure

- 45% of respondents from critical national infrastructure are experiencing an increase in the volume of attacks on their network.

Volume of attacks on the network

Respondents from critical national infrastructure



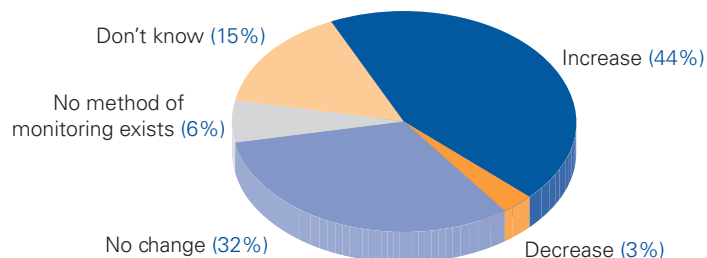
- 51% of respondents from critical national infrastructure indicated an increase in the technical sophistication of attacks on the network.

It is by no means the case that critical infrastructure as a whole is currently under sustained assault. However, when considering attack patterns on networks belonging to critical infrastructure, responses would seem to indicate a parallel increase in volume and sophistication against such targets. A significant amount of industry-specific knowledge therefore exists within the cyber-criminal community on security protocols, response tactics, and weak-points.

- 44% of respondents from critical national infrastructure registered an increase in specifically targeted e-Crime attacks on their network.

Volume of specifically targeted e-Crime attacks on the network

Respondents from critical national infrastructure



Some respondents from critical infrastructure indicate that criminals are testing multiple weak points, taking more time to plan and execute attacks rather than exploiting individual flaws as they emerge.

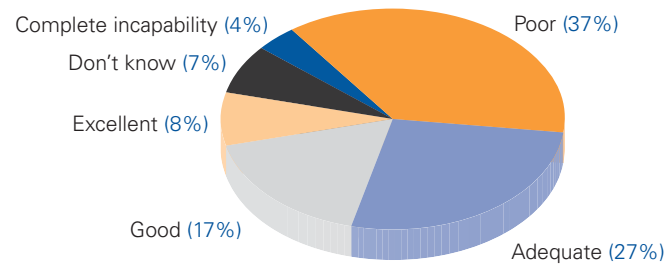
A potential aggressor could, with the right connections, draw upon this resource. If access to insider knowledge of weak-points was available it can reasonably be concluded that a well-planned, hostile attack on specific industries, (or across the board), would have the potential to be massively damaging.

- Only 17% of respondents from critical national infrastructure classify the capabilities of the country they operate in to coordinate an effective response against a major and concerted hostile attack against systems

that comprise critical national infrastructure as “good”. 37% classify it as poor.

How would you assess the capability of the country you operate in to coordinate an effective response if a major and concerted, hostile electronic attack targeted vital computer networks that make up the critical national infrastructure?

Respondents from critical national infrastructure



In 2008 and early 2009, three separate nations were targeted by large-scale hostile Internet-borne attacks; Estonia, Georgia, and Kyrgyzstan. The validity of the term “cyber-war” is a contentious issue within the security community. However, what is certain is that these attacks were of a different breed to those with a distinct business focus.

The accepted wisdom has been that cyber-criminals would not engage in massive disruption of Internet services because they rely on a functioning web to execute attacks. However, the validity of this assumption must now be questioned. Massive botnets, (either active or redundant), are in the hands of groups who are driven by financial motive. Supposing that services would not be made available to the highest bidder, regardless of the purpose, would be a dangerous second guess.

Although the impact of large-scale attacks has highlighted the need for cyber-defence protocols to be put in place, coordination of such frameworks is a problematic area that defies an easy outcome. The main barrier to a solution is ownership, both of systems and responsibility.

From the frontlines...

What worries you most about attack trends in terms of the threats with the greatest potential to impact your organisation financially?

- Organised terrorist attacks combining physical and cyber vectors.
- That our operational capability to deal with large-scale attacks will be overwhelmed.
- Botnets will continue to increase in size, complexity, and ability to knock things over.
- Increasing likelihood of state actors undertaking attacks.

■ **While 22% of respondents from critical national infrastructure are already coordinating a response framework in partnership with other organisations, 25% indicate it is “not very likely” that coordinating with other industries against such an attack will be a priority for their organisation in 2009.**

In the majority of cases, government no longer controls critical infrastructure. This may not be the case for financial services companies that are being part or wholly nationalised, but there are more pressing problems for government in this domain than reviewing resilience in the event of a massive and targeted hostile cyber-attack.

In reality, government has little or no control over the methodologies used to benchmark security measures, or on what basis risk is assessed. Short of instituting a cyber-defence compliance standard, there is no way industry can be

forced to prioritise a holistic concept that does not lend itself to being easily understood by a board of directors who are concerned with delivering value to shareholders.

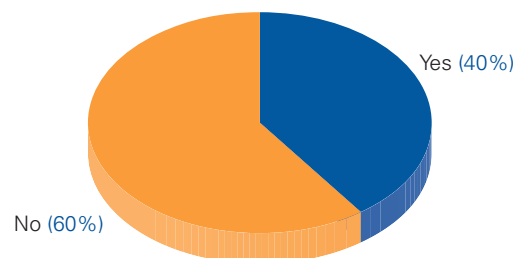
Even if a cyber-security standard was brought into existence companies would have to go through an exhaustive mapping exercise similar to that necessary for business continuity planning, but with added complexities and variables. Such a task would take an inordinate time to complete. It would also require constant monitoring to take into account new interdependencies that affected strategic oversight of operational integrity, such as those created by outsourcing.

That the greatest number of respondents feel they are unlikely to coordinate with other industries is perhaps not surprising in this context. Considerations such as protection of customer data can be easily framed in terms of negative publicity, decreasing stock value, regulatory fines, and damage to reputation. At executive level cyber-defence is likely perceived, if indeed it is understood at all, as an issue for the security services and the military.

- **The majority of respondents from critical national infrastructure have not reviewed the defence and response capabilities of business partners and service suppliers.**

In the last 12 months, have you carried out a risk assessment of your business partners and service suppliers to establish their defence capabilities and response framework in the event of a major and concerted hostile electronic attack on their computer networks?

Respondents from critical national infrastructure



Businesses comprising critical infrastructure may be confident of the ability to defend their own critical systems in the face of a hostile attack. However partners, vendors, and suppliers who deliver first or second tier services may not be so prepared.

External dependencies and an increasing spectrum of international partnerships have increased the functional connectivity of geographically dispersed systems. For this reason, the ability to maintain operational integrity could easily be reduced to that of the least resilient service supplier. Equally, indirect attacks may provide hostile attackers with another method of compromising critical systems.

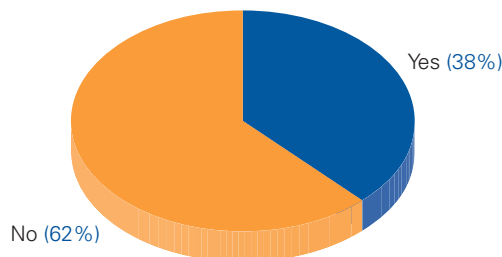
Key findings: On the business of security

Mind the gap

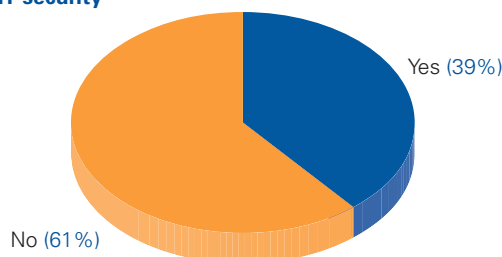
- 62% of respondents do not believe their organisation dedicates enough time, budget and resources to locating vulnerabilities.

Do you think that your enterprise dedicates enough resources, budget, time, and effort to finding and resolving weak-points in technical processes when you consider the resources and capabilities of the cyber-criminal community in locating and exploiting vulnerabilities?

All respondents



Respondents from IT security



From the frontlines...

What worries you most about attack trends in terms of the threats with the greatest potential to impact your organisation financially?

- The fact that there are vulnerabilities in all kinds of software. There are no longer "safe" file formats as pdf-files, jpg, gif etc can be used to exploit vulnerabilities in software.
- Vulnerabilities in used infrastructure (software, networks, operating systems).
- The plethora on unofficial and unapproved software installed on user computers and PDAs/XDAs multiplies the exposure to malware attacks but only official software installations are considered.

The opinions and concerns voiced by respondents indicate that organisation-wide awareness of security risks has not kept step with the evolution of e-Crime threats. It could be argued that this majority may not indicate businesses are lackadaisical in their responsibilities, but simply that those who spend their time "doing security" think greater emphasis should be placed upon it. Far more likely, this statistic implies respondents do not believe that a high enough percentage of business stakeholders are cognisant of what "risk" really means in the electronic age.

The number of applications and technologies in the enterprise environment will continue to increase exponentially. The pace and scale at which new products are adopted in pursuit of greater competitive advantage, or in search of business processes optimisation, has opened a Pandora's box of security vulnerabilities for organisations of all shapes and sizes.

- **Only 14% of the total number of respondents indicated that "Requirement to secure new business technology" was a reason for increased investment in security capabilities over the past year.**

However, it would seem that securing new technologies is neither driving increases in security budget nor even sitting in the passenger seat. If comprehensive considerations of security implications is a rare occurrence when implementing new technologies, or indeed when planning their design, risk is consequently multiplied. That vulnerabilities exist is a huge problem but when the owners of enterprise processes have no knowledge about potential weaknesses, (the unknown unknowns), susceptibility to attack is far greater.

Aces and eights

This driver highlights a common misconception of security as a point solution, and not as the ongoing process that it is. Those organisations that do not invest in security until aware of high-profile incidents are likely to be more vulnerable than their security-prudent competitors – increased time between system security updates (whether through patches or configuration changes) increases the potential attack surface. This becomes a self-fulfilling prophecy for those organisations that act only upon awareness of incidents, never really addressing the core issues and therefore never deriving adequate levels of assurance over their systems and networks.



Spending trends

- **High-profile incidents in other organisations was selected by the greatest number of respondents as a main driver for increased investment in security capabilities.**

After a year of high-profile data breaches, culminating in Heartland Payment Systems’ disclosure in early 2009, it is hardly surprising that the area identified by the most respondents as contributing to an increase in budget was “incidents in other organisations”.

- **The driver with the second highest response rate for increased investment in security capabilities was regulatory compliance.**

While broad-sheet coverage of breaches may flag the issue of data security with board members, (and provide a good opportunity for security professionals to use others’ failings as scare tactics), the spectre of regulatory compliance and the threat of financial penalties for losing data is also a clear motivator.

Winners PODIUM by all respondents

The main drivers for increased investment in security capabilities over the past year†

1st	High-profile incidents in other organisations	42%
2nd	Regulatory compliance	41%
3rd	Fear of a major incident resulting in negative media coverage of your organisation	40%

By industry

Driver identified by most respondents from finance:	Regulatory compliance
Driver identified by most respondents from government:	High profile incidents in other organisations
Driver identified by most respondents from retail:	PCI DSS
Driver identified by most respondents from oil and gas:	Impact of an internal security incident or external attack

† Percentages shown indicate a proportion of total responses.

- **67% of respondents selected “Budget” as a major bottleneck preventing their organisation from increasing proactive capabilities to reduce the impact of e-Crime.**

That so many respondents indicated that spending was motivated by reports of others’ misfortune strongly indicates that a reactive security posture still exists in many large enterprises.

Responding to existing threats is the priority for the majority, and rightfully so. However, with insufficient resources to build proactive processes, the chances of getting ahead of the attack curve are much reduced. However, it would be wrong to assume that the business is not listening. The second greatest bottleneck identified was “Difficulty providing a credible threat forecast that demonstrates the possible business impact of future attacks”, selected by 39% of respondents. Perhaps the difficulty of communicating this, or a lack of imagination on the part of those to whom risk is communicated, is why organisations will continue to have to suffer before security is taken seriously.

From the frontlines...

What worries you most about attack trends in terms of the threats with the greatest potential to impact your organisation financially?

- No budget to run a project to do the next phase of the IT security programme.

From the frontlines...

What worries you most about attack trends in terms of the threats with the greatest potential to impact your organisation financially?

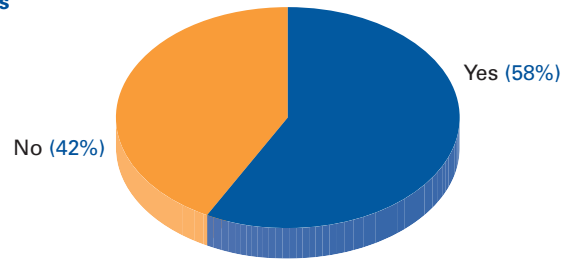
- Loss of compliance leading to fines.
- Potential sophisticated hardware compromise of Pin entry devices (chip and Pin).

The PCI DSS

- **Of respondents who have to comply with the PCI DSS, 58% say that it has contributed positively to the visibility of IT security at board level while 42% say that it has not.**

Has the PCI DSS (Payment Card Industry Data Security Standard) positively contributed to the profile and visibility of IT security at board/executive level within your organisation?

All respondents



The Payment Card Industry Data Security Standard would appear to have had a divisive effect on those who have to comply with it.

For one industry sector however, it has provided the necessary impetus for investment in security and has had a positive effect on how they are perceived by the board.

- **Of those respondents from retail who had to comply with the PCI DSS, 92% indicated the PCI DSS had contributed positively to the visibility of IT security at board level.**
- **90% of respondents from retail selected “Compliance with the Payment Card Industry Data Security Standard” as one of the main drivers for an increased investment in security capabilities over the last year.**

There is a spectrum of possible reasons that a percentage of respondents chose “No” when asked if PCI had had a positive impact. They may already enjoy a high level of visibility at board level. Conversely, security managers may be troubled that senior executives see no need to invest in measures that go above and beyond what the standard demands.

The standard has gone a long way towards establishing a common baseline for IT and information security. However, when considering the issues raised in this survey regarding the threat from malware and the concerns of security practitioners, it may be suggested that to consider PCI DSS compliance a watertight guarantee that data is protected and that systems are safe from infiltration would be at odds with the risk landscape.

Governance and proportionate security

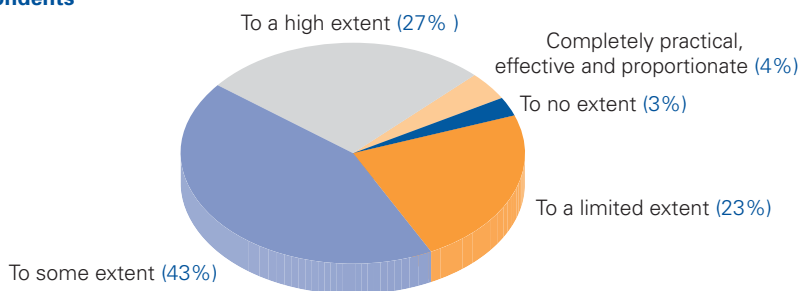
- **70% of respondents registered that the Board of Directors considers their department to be an integral part of corporate planning, governance and enterprise risk management with regards to business strategy and the development, implementation, and maintenance of infrastructure.**

The role of security departments is changing, and the fact so many respondents indicate that their departments are central to business strategy is highly encouraging.

Applying the breaks on commercial objectives is no longer the modus operandi of the security professional; there is a growing trend to act as a business facilitator, consciously keeping costs low, adding to the bottom line wherever possible, and enabling diverse projects to achieve their objectives while keeping exposure to risk at an acceptable baseline.

When you consider the threat to the targets you have identified, and the difficulties associated with balancing real and assumed risk, to what extent do you feel your organisation's security strategy is practical, effective, and proportionate?

All respondents



When compared with this result, the range of feeling about whether security strategy is practical, effective, and proportionate perhaps reflects the pitfall to adopting this posture. As the threat matrix becomes ever more complex, security practitioners may find themselves torn between the business impact of not applying the breaks and the internal implications of doing so.

- **The majority of total respondents, 62%, feel that their organisation thinks outside the box to some extent.**

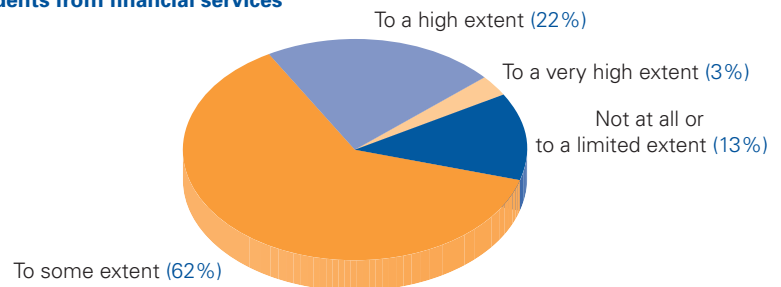
Technological innovation will not stop, new applications will be unleashed upon the business environment, and security will only become more critical to the integrity and availability of business services. As innovation continues to provide cyber-criminals with new routes of attack, lack of risk awareness multiplies the number of vulnerabilities that can be successfully exploited.

Thinking outside of the box is key when predicting how attacks might change and evolve. Security stakeholders, more than most, understand the need to think holistically about process exploitation and the importance of carefully

considering the opportunities for malicious targeting of business units that rely on a spectrum of enterprise systems.

To what extent do you think your organisation thinks 'outside the box' when conducting risk assessments of processes and technologies which can be targeted by cyber-criminals?

Respondents from financial services



A mounting challenge for security professionals will be the extent to which their peers in other departments understand the nature of the threat from e-Crime. Actively engaging end-users in the business of security relies on effectively educating them. The key questions are: What do you educate them about?; How do you clearly communicate electronic threat in a language that they understand?; How can you maintain a sufficient level and consistent level of security awareness bearing in mind the range of departments who have a part to play?.

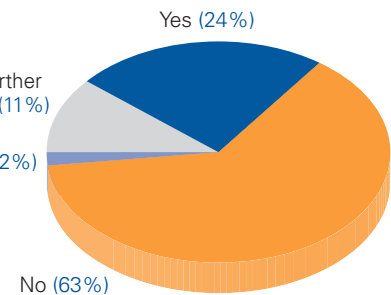
Spotlight on data protection and investigation laws

Does your company's lack of clarity over data protection and investigation laws hinder your ability to investigate cross border incidents?

All respondents

As it is too difficult we do not progress matters further in countries that enforce strong data privacy laws (11%)

We ignore the laws (2%)



The indications from the survey are encouraging in that over 60% of respondents don't think that cross border investigations are hindered. Just under a quarter of companies find that DPA hinders their ability to investigate incidents and some 11% do not progress matters, potentially leaving the causes of security incidents unresolved and the business exposed.

In a recent white paper prepared by KPMG Forensic more than 45% of companies surveyed found that the top challenge to conducting cross-border investigations was the legal or regulatory environment including the data protection acts. In any cross-border investigation it is vital that consideration is given to evaluating the organisations IT structure and location of the data such that local laws are considered. The local laws and guidance will differ widely from those where the headquarters of the business is located. In order to avoid problems with such matters it is important for companies with overseas operations to ensure that those likely to be dealing with the investigation are fully aware of the local laws where data is stored. Areas to be considered may include:

- The attitude of local authorities to "overseas" controlled businesses operating in their country.
- What is legal in one country may be custom and practice in another.
- The extent to which the local authorities will expect, require or pursue prosecution.
- How evidence that has been gathered may be used in court.
- The evidence required to secure a successful civil outcome or criminal prosecution.
- Individual data privacy laws.

Companies must ensure that they understand relevant international and in-country legislation to avoid committing any offence during the investigation. If the correct steps are not taken during the course of the investigation of a cross border incident difficulties could result going forward.

The challenges associated with conducting cross-border investigations are complex, lending weight to the imperative for being properly prepared. The landscape is a constant shifting entity, which will continue to give rise to new threats. Being ready to respond with a flexible approach will best prepare companies to react to meet the challenges of investigating cross-border incidents.



The greatest barriers to sharing actionable intelligence between law enforcement, government, and business on e-Crime in a timely manner are identified as

- **Trust** in what will be done with the information.
- **Locating an appropriate point of contact** in external organisations.

Cyber-criminals operate in a joined-up world.

They are able to share information easily, quickly, and confidentially on which attack techniques are effective.

Products and services used to target businesses and their customers are easily accessed, cheaply purchased, rapidly distributed, and increasingly sophisticated.

The constantly evolving landscape of risk associated with e-Crime continues to expand at the same relative speed as the technologies that make it possible.

Phone +44 207 831 7545 and find out how you can get ahead of the curve.

Summary and conclusions

Innovation in a forgotten era

In the days of the Wild Wild West, Jesse James' gang conducted countless successful bank hold-ups across a wide territorial area. For a time, the pattern of attack provided rich rewards with low risks. However, when a combination of increased vault security and armed civic defence forces came into play, largely in response to the success of the gang, the balance shifted in favour of failure.

The unacceptable odds of capture, (or more unappealingly, death), meant that the James gang had to innovate. They duly turned their talents to the railroads, and after a first botched attempt, they succeeded in netting a total of \$3,000 in the world's first robbery of a moving train.

Criminality in the age of the wild wild web

E-Crime is not a threat that can be solved by compliance or the deployment of technology. Its prevention is, and will remain, a strategic issue.

Without exception, managing security at enterprise level in the 21st Century is a task that brings with it unique challenges, not least of which is how best to proactively protect profits and operations in a rapidly changing commercial environment.

To be certain to take what you attack, attack where the enemy cannot defend.

SunTzu, The Art of War

Those interested in the interplay of defensive and offensive strategy during conflict may be familiar with the Sun Tzu, or the Art of War. This text is widely regarded as a definitive guide to understanding the dynamics that govern conflicts and decide their outcomes.

When interpreted in the context of e-Crime, this verse offers three stark warnings.

Firstly, methods of attack will always innovate in line with the defences that are deployed. In order to be sure of success cyber-criminals will determine the point of least resistance, rather than look to bypass existing security barriers.

Secondly, where there is inherent vulnerability in a process or series of processes, it is not necessary for the weapon to be sophisticated in order to achieve your aim. It is simply necessary for the victim to be unaware that they are at risk, or overconfident of their defensive ability.

Finally, cyber-criminals will continue to target the one area that neither business, nor government or law enforcement can protect: the online consumer.

Postscript

Post analysis of the recent e-Crime survey statistics, a number of factors jump out from the findings. First of all, notwithstanding the perception that e-Crime is actually on the decline, the reverse seems to be the case.

Secondly, there are indications that the green shoots of inter-corporate awareness of the threats posed by e-Crime are increasing, and we see many more security professionals plugged into understanding the profile of next generation threats. However, there is also a suggestion that whilst the level of appreciation of the security professional is enjoying a spurt of growth, it would seem this is yet to filter through to manifest as board level recognition and support.

Based on recent events in which we have seen the collapse of the economy unfold, largely based on "light touch" governance, fraud and aspects of insider trading and dealings would seem to have been rife. We also see a large number of organisations surfacing who would seem to have suffered insufficient internal controls – which can only infer the insider threat is more significant than anyone could have thought possible.

Link this to reports of breakdowns in system security, leading to easing the path for Housing Fraud, and it may be strongly inferred that we are yet to find out more. To quote Lord Mandelson from his address to the City Trade Investment Dinner (Mansion House March 2009); "We used to talk about light touch: now its going to be about the right touch".

Time will only tell just how bad the state of e-Crime and related matters stand, but one thing is for sure. It would certainly seem to be the only growing industry of the current day!

Professor John Walker

Director, ISSA International Board

5 March 2009

Contact details

The editor, Jonathan Hawes, can be reached at jon.hawes@akjassociates.com

© 2009 AKJ Associates Ltd.
All rights reserved. Neither this publication nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical photocopying or otherwise without the prior permission of AKJ Associates Ltd.
e-Crime Congress is a registered trademark of AKJ Associates Ltd. Other names may be registered or non-registered trademarks of their respective owners.

© 2009 KPMG International.
KPMG International provides no client services and is a Swiss cooperative with which the independent member firms of the KPMG network are affiliated.

About AKJ Associates

AKJ Associates is a business information company that specialises in providing strategic and technical guidance in the areas of corporate risk and security management, and public sector security strategy.

Our reputation as the leading provider of events on risk and security matters has been earned over a decade of hosting global forums and organising bespoke initiatives. During this time we have worked closely with senior representatives of business, government, intelligence agencies and law enforcement, as well as the market's leading service suppliers.

Events hosted by AKJ Associates are renowned for providing senior level delegates with cutting-edge solutions and examples of best practice, as well as access to exclusive peer-to-peer networks. The content of our initiatives is specifically designed to deliver strategic guidance, innovative thought leadership, and technical insights to those within national and global enterprises who are tasked with managing security, IT, risk, audit, investigations, fraud, forensics, operations, and asset protection.

Our current portfolio focuses on electronic crime, the protection of intellectual property in electronic environments, electronic discovery and forensics, asset protection, internal investigations, regulatory compliance and the PCI DSS, business continuity, and enterprise resilience. Across this spectrum of topics, we are known for facilitating and consolidating working partnerships between providers of security solutions and the world's largest corporations, national policing and intelligence agencies, and international governments.

www.akjassociates.com

About KPMG

KPMG operates as an international network of member firms offering audit, tax and advisory services.

We are one of the world's leading providers of audit, tax and advisory services with more than 137,000 people operating in 144 countries worldwide.

We help our clients to fight e-Crime by working closely with them to prevent, detect and investigate incidents and by mitigating their impact.

In this document "KPMG" refers to member firms of KPMG International, a Swiss cooperative.



Disclaimer

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Notes

One of the world's most influential forums on combating cybercrime is expanding...



**Mumbai, India
November 2009**



Over two days the e-Crime Congress India and Asia Pacific will address key challenges for security professionals who are responsible for protecting their enterprise systems and their customers from an increasingly sophisticated and malicious threat.

The event will host senior decision-makers and security professionals from the Asia Pacific region and address key challenges for companies operating in countries that include Australia, China, India, Japan, Malaysia, New Zealand, Philippines, Singapore, South Korea, Thailand, and Vietnam.

The information security landscape is experiencing profound changes as new ideas, new standards, and regulations reshape the collective thinking on technological threats and deterrence in a constantly connected global society.

As the technology risk landscape has evolved from amateur virus-based attacks into a threat matrix that is highly organised, well funded, and professionally executed, so too the needs of business and government have changed.

By providing strategic and technological solutions that can be deployed to protect against existing attacks and emerging threats the e-Crime Congress India and Asia Pacific will promote best-practice for e-defence.

e-Crime Congress India and Asia Pacific will welcome delegates from India and the Asia Pacific Region.

Typical job titles of those attending will comprise:

CXOs • Business Strategists • Enterprise Architects • Global and Regional Security Leaders • IT, Fraud, Risk and Technical Directors • Analysts, Research, and Business Intelligence Professionals • Law Enforcement Heads of Hi Tech Crime • Senior Government and State Government Officials • Policy and Regulatory Representatives.

Delegates will attend from a range of industry sectors including:

Banking • Communications • Construction • Education • Energy • Engineering • Entertainment • Finance • Government • Health • Information Technology • Insurance • ISPs • Law Enforcement • Legal Practices • Manufacturing • Media • Military/Defence • Mining • Pharmaceuticals • Professional Services • Retail • Telecommunications • Transport • Travel • and Utilities.

**For more information, please phone +44 (0) 20 7430 9250
or email howard.james@akjassociates.com**



Your exposure to electronic crime may be greater than it first appears.

Electronic Crime can weaken a company's foundation.

KPMG member firms' IT Advisory teams can help you identify threats to your organisation and navigate a safe path through the application of sophisticated technology tools and consistent methodologies.

We can help simplify complex issues: explain threats to your business, advise on the application of compensating controls and embed processes to help ensure consistency.

Our services are delivered by professionals with strong IT security and business process skills ready, able to assist you on a global level.

We can help you to keep your reputation on high ground.

Call Malcolm Marshall from KPMG in the UK

Tel: +44 (0)207 311 5456

e-Mail: malcolm.marshall@kpmg.co.uk

kpmg.com/forensic