agn INTERNATIONAL

Cyber Security: The international threat to business continuity

Global Business Voice: The AGN Global Survey of issues that impact national businesses and the SME

excellent.
connected.
individual.

Cyber Security

It's tempting to give in to ransom demands, but better to resist them

The largest and arguably most powerful ransomware attack the world has seen started to infect IT systems on Friday 12 May. The 'WannaCry' virus threw organisations in the UK, US, Russia, Germany, China and more into meltdown: 157 countries were involved in the attack.

We've since seen additional ransomware attacks at the end of June and in August. Digital threats – long spoken-about as a potential risk – are now a day-to-day reality that organisations must face.

Welcome to the third AGN Global Business Voice Survey. In this issue we look at the recent AGN Global Business Voice (GBV) opinion panel discussion on cyber security, and how ready the panel's clients are for future attacks.

Many companies think it's easier just to pay up (Q1)

US companies paid out $1bn in 2016 to ransomware blackmailers, according to FBI estimates.

WannaCry demanded victims pay between $300 and $600 to gain access to their critical systems. It's a smart and carefully considered amount: not enough to hurt a business's ongoing operations, and perhaps less than the resources it would take for a business to report or avoid it. But overall these small sums add up to a very big number: a recent Hiscox report estimated that the cost of cyber crime on the world economy amounts to $450bn every year.

Some 40% of companies advised by the AGN GBV panel – equating to tens of thousands of companies worldwide – have been affected by WannaCry or some other malware virus in the last 12 months, though not all companies paid up.

Malcolm Ward, CEO for AGN says: "The amount of money paid out to ransomware criminals is really the elephant in the room. Individual amounts can be modest, but in aggregate, companies are giving billions of dollars every year to these hi-tech blackmailers."

Businesses aren't prepared for malware – more education is needed (Q2)

The panel generally felt their clients were ill-prepared for cyber attacks. The panel suggested that 58% of their clients only had a moderate awareness of the potential threats posed by malware attacks, and another 29% have low or no awareness at all.

Malcolm Wards says "There is clearly still an education job to be done here. It's not surprising that businesses are ill-equipped to deal with malware when so few actually understand what an attack could do to their business, and the crippling effect it could have."

It's costing businesses substantial sums, in time as well as money (Q3)

40% of the GBV panel thought that some of their clients had suffered a cost due to cybercrime. 18% of the panel said that between 2% and 5% of their client bases had suffered financially, and another 22% thought that up to 1% of their entire client base had suffered a material cost. 58% of clients haven't yet suffered financially.

Malcolm Ward stated: "There is of course a direct cost in terms of paying out any ransom demand, but there are also costs associated with downtime and disruption that can run into days, weeks or even months depending on the nature of the attack. These costs can run into thousands or millions of dollars, or even threaten an organisation's very survival."

Companies still aren't getting advice…but that must change (Q4)

Only a small proportion of the panel's clients are getting professional cyber security support: 80% of the panel reported that less than half of their clients were taking professional cyber security advice.

Malcolm Ward: "Cyber security is a relatively young industry. There is too little awareness of cybercrime, and a bewildering array of problems and professional solutions that can be inaccessible to the layman. But the market will mature and businesses will look closely at managing and mitigating the risks involved."

What accountants and advisers should do for their clients' cyber security (Q5)

All of the panel recognize that accountants have a role to play in advising on cyber security, and over 70% think that role is either 'critical' or 'very important'.

"The responsibilities of the auditor, accountant or financial adviser are complex and depend on the nature of the individual assignment. However, engagements will often involve understanding the clients business, the key risks its facing and the adequacy of controls management has in place. Given the low awareness and difficulty of accessing advice, this is where accountants need to ensure that cyber security issues are front of mind as they go about their work, and help their clients focus on the area and manage the risks." Malcolm Ward, AGN CEO.

In Conclusion

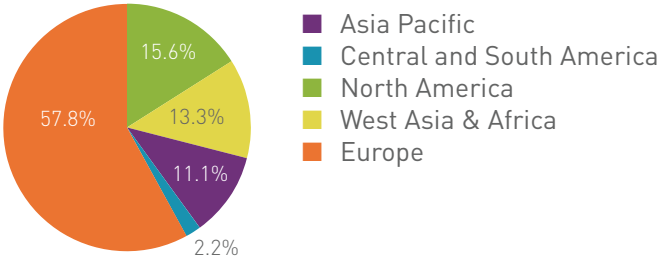
- The frequency of cyber attacks on businesses is increasing but awareness is low and advice seems difficult to access.
- Individual sums lost to ransomware are usually small but they're combining to become a big problem.
- As more businesses face this extortion more frequently, it's likely that the market for solutions will evolve and mature.
- But right now, there is a risk that businesses are not taking this threat seriously enough, and not taking the right advice to manage risks and control the consequences.

"It's not clear that businesses are thinking of cyber risks as an immediate and urgent business continuity issue. Few will operate without insurances and contingency plans for physical events like fire or flood, but arguably the risk to business from cyber attack is both more likely and harder to assess and plan for. Accountants need to step up: encourage their clients to evaluate and plan for these risks, and support them in doing so." Malcolm Ward, AGN CEO.

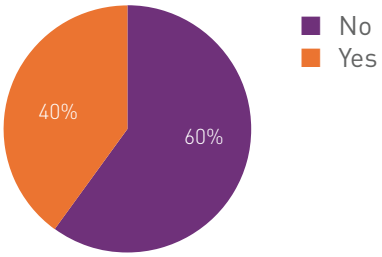
Survey results

45 responses

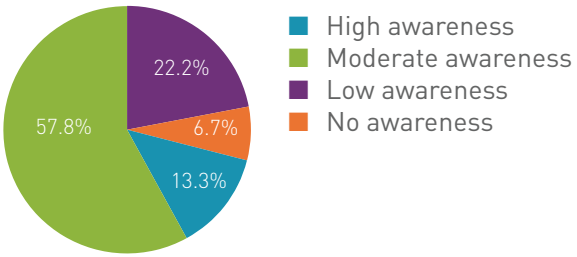
Participant's region:



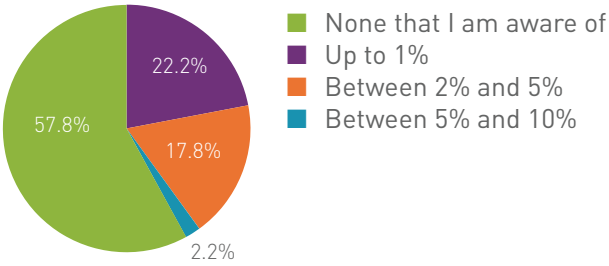
Q1: Are you aware of any clients being affected by the recent Wannacry malware virus or any other similar external attack in the last 12 months?



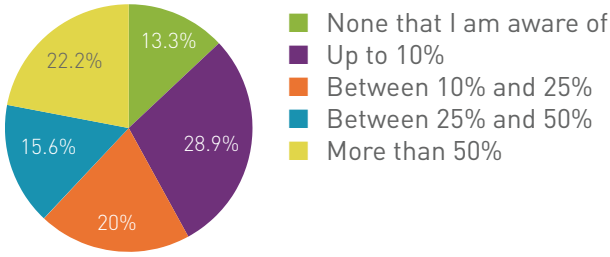
Q2: How do you rate your client's levels of awareness of the threats posed by cyber fraud or attacks?



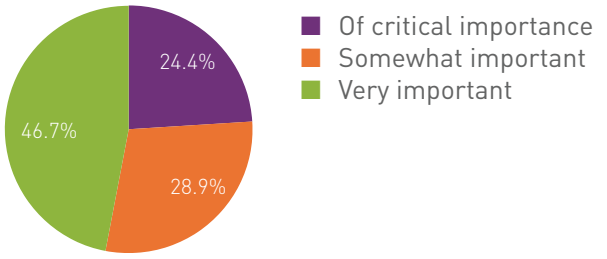
Q3: Approximately what proportion of your clients do you estimate suffered financial loss due to cyber fraud or attacks in the last 12 months?



Q4: Approximately what proportion of your clients do you estimate receive specialist professional advice regarding cyber security?



Q5: As accountants and advisers how important is our role in advising clients of cyber security risks and practices?



excellent.
connected.
individual.

For further information, or become involved, please contact:

AGN International
Email: info@agn.org | **Office:** +44 (0)20 7971 7373 | **Web:** www.agn.org