Grant Thornton
An instinct for growth™

Information Security

Cyber Security Survey - Results

Grant Thornton's summer 2018 cyber security survey of Channel Islands organisations produced some intriguing and in some cases surprising results.

September 2018

Contents

About the author

David Cartwright
Senior Consultant, Information Security

Experience

David has over 20 years' experience in IT, networking and telecoms, and specialises in information security. He has worked in the Channel Islands since 2007. He holds CISSP, GDPR Practitioner and ISO 27001 Lead Auditor qualifications, along with FBCS, CITP and CEng professional status.

He is presently Chairman of the Jersey branch of the British Computer Society, and Vice Chairman of the Channel Islands Information Security Forum.

T +44 (0)1534 885813
E david.cartwright@gt-ci.com

Introduction

The cyber security statistics we see most often tend to relate to data breaches: where targeted attacks or indiscriminate malware have infiltrated IT systems and have made sensitive, confidential data accessible to those who have no right to see it.

Our short survey took a more pragmatic look at how cyber security is handled in the Channel Islands. While the first thing we asked was the fairly inevitable question of whether organisations had experienced a breach in the last year, we were more interested in what the perceived threats are, and what organisations are doing – and plan to do – about them. What do they intend to do in the coming months to protect themselves? If they have a problem, what do they think the likely cause will be? Are security certifications important, and how many organisations have them? How do they keep up with new threats, and what do they do to keep their staff informed?

In short: we see major security breaches globally, but what are Channel Islands organisations doing to understand the problem and protect themselves against being the next to hit the front page?

Information security is not, fundamentally, rocket science. While it's certainly true that the intricacies of some of the attacks that go on around the world are complex, most security breaches are made possible because of simple mistakes. A user is fooled by a 'phishing' campaign and gives away his or her username and password. A hacker breaks through your firewall by exploiting a known vulnerability, because nobody installed the software update that would have prevented it. An intruder accesses confidential documents in a building because we're brought up to be polite and someone holds the door open for them.

As we see from this report, the threats seen by the respondents are many and varied, and a multitude of approaches are taken when dealing with them: installing technology and training staff; obtaining security certifications or simply aligning operations with known standards; expanding internal security teams and taking advice from external consultants.

There's no one right way to keep your organisation secure: a good security regime has multiple components, operated robustly. We hope this report gives a view of the attitude taken around the Channel Islands, and provides a guide as to where you should be looking in your organisation.

Headline results

Half of business are certain they haven't been hacked

We asked: Have you had a security breach in the last 12 months? **49%** of respondents answered with an emphatic "No". A more cautious **26%** said "We don't believe so". One of the hardest tasks in cyber security is detecting that your systems have been compromised, so such a high level of confidence is encouraging – if indeed their beliefs are correct.

Of those organisations that said they had had a security breach, the most common – **13%** - was accidental user error.

Over two thirds of businesses train all their staff on cyber security

It's acknowledged that people are the biggest threat to an organisation's security. No matter how hard you try, people will make mistakes – along with **13%** of attacks in the last 12 months being due to user error, two thirds – **67%** - of respondents predicted that user error was the most likely reason for them to have a breach in the next year.

It's reassuring, then, that **69%** of respondents said that they give information security training to all staff at least annually, and **59%** intend to do so in the next year. On the negative side, though, **28%** don't do any regular training at all.

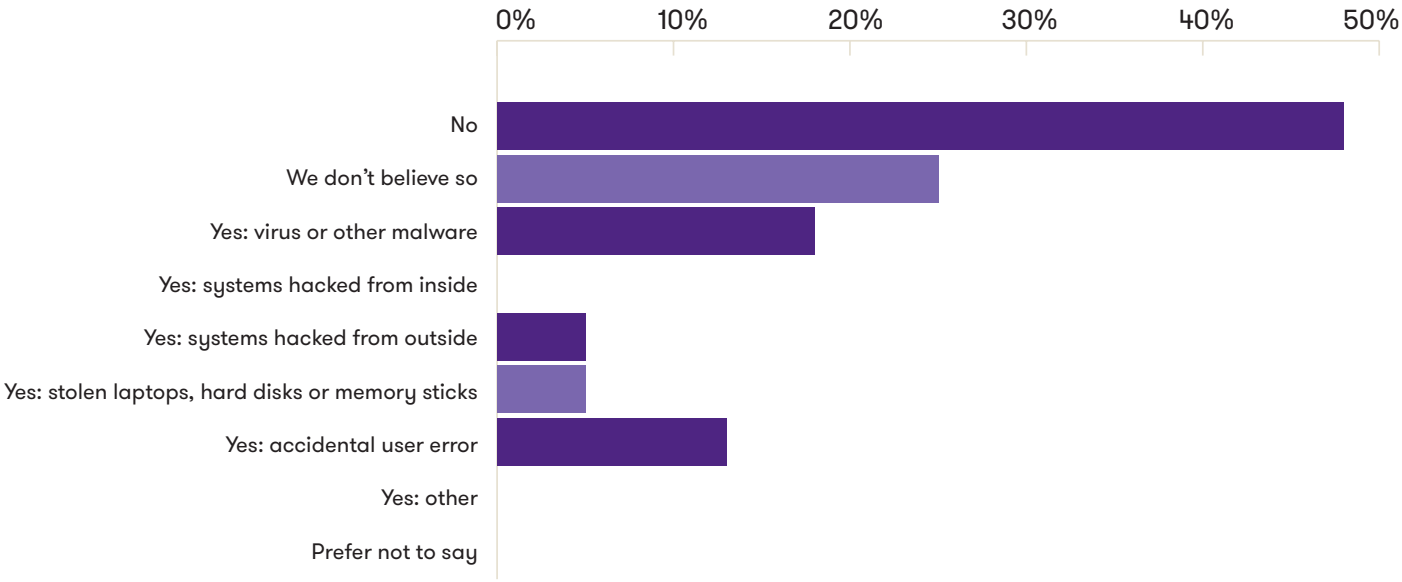
Crucial security standard adopted by only 8% of businesses

Cyber Essentials is an excellent certification scheme: organisations that comply with its requirements protect themselves against the vast majority of potential attacks.

The UK government already mandates Cyber Essentials for most of its suppliers, and the States of Jersey will follow suit in 2020. Yet only **8%** of respondents hold Cyber Essentials certification, and **37%** hold no security certifications at all.

Detailed results

Have you had a security breach in the last 12 months?



Results

Three quarters of respondents said that they'd not experienced a security breach in the last year: **49%** were certain, while a further **26%** said that they'd not had a breach as far as they were aware. Of those who had experienced issues, the most common was accidental user error at **13%**. Stolen equipment and external hacks were equal, at **5%** each, with no respondents reporting internally perpetrated hacks.

Recommendations

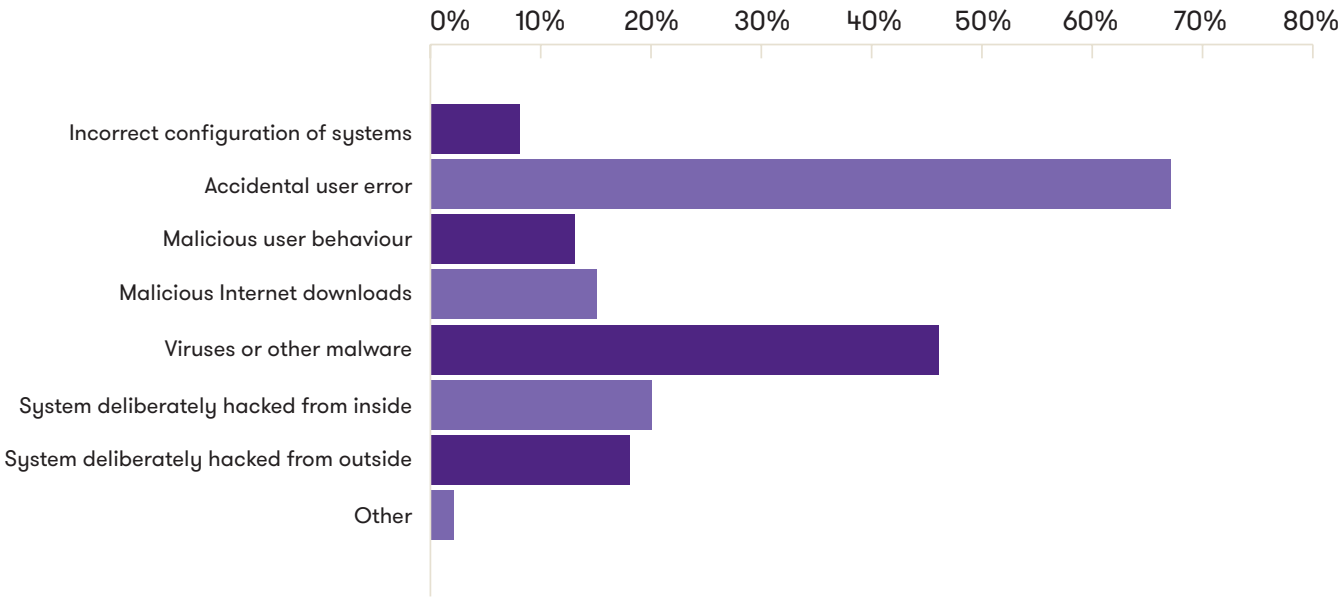
It's absolutely essential to **log and monitor all the systems** that can give clues to cyber attacks, and to make those logs tamper-proof so an attacker can't cover his/her tracks. A Security Information and Event Management (SIEM) solution is a great option if you have the resources and knowledge, but even if you can't justify one there's no excuse for not monitoring activity. And look at the outputs regularly: there's no point generating loads of data that could help you spot a breach if you don't bother looking at it.

Testing is also crucial. Even small companies should have some kind of penetration test at least once a year, and larger organisations and/or companies with sensitive or personal data accessible from the Internet (e.g. online shops, customer portals and the like) must have in-depth pen tests, preferably no more than six months apart. No matter how well you think you've configured your security, the only way to prove this is by testing.

Internal testing should also be part of your test regime. If an intruder gets through your perimeter, you need to minimise the damage they can do by jumping from system to system internally.

Detailed results

If you were to experience a security breach in the next 12 months, what would be the likely cause(s)?



Results

This was a fascinating category, with the vast majority (67%) of respondents believing that accidental user error would be the cause of security issues in the coming year; although malicious user behaviour is on some people's radar, it scored significantly lower (13%) than accidental user breaches. Almost half (46%) are expecting problems from malware, with 15% fearing dodgy file downloads. Although nobody reported experiencing internal attacks in the previous question, 21% think they're likely to experience one in future – which perhaps surprisingly is slightly more than the 18% who expect an external hack.

Recommendations

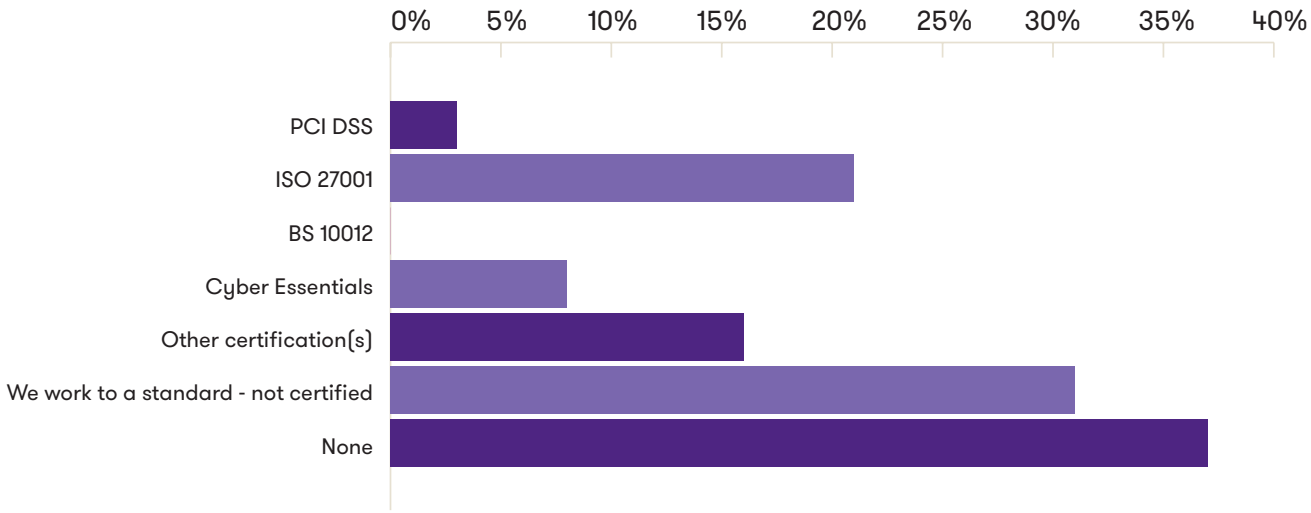
User awareness training is inexpensive and always beneficial. Experience has shown us time and time again that a couple of instructor-led sessions per year, supplemented by short monthly email updates, causes user reports of suspicious activity to go up and the number of user-induced breaches to go down. Every time.

Anti-virus/anti-malware protection is absolutely mandatory. Make sure all devices are protected, and that they update their virus signatures at least twice a day (preferably more). If you can, use an enterprise-grade product (all the main anti-virus software vendors have one) where your devices are monitored via a central console, as this gives you a single point of reference of how up-to-date the systems are and which have had attempted attacks.

Discipline as a last resort: you can't get people to admit making a mistake (falling for a "phishing" scam, for example) if they think they will be disciplined for it. Build a culture in which people are encouraged to report mistakes, reminding them that if they tell you about it, you can help fix the problem and mitigate the risk. Discipline's necessary for malicious behaviour, of course, but don't scare people off reporting that they did something wrong.

Detailed results

Do you have any other security certifications?



Results

Over a fifth (21%) of respondents say they hold ISO 27001 certifications: this seems high, but may be attributable to natural skew (that is, respondents to cyber security surveys may tend toward those who are interested in the topic and are hence more likely to have sought and obtained certifications). With this logic, then, it is perhaps more surprising that only 8% hold Cyber Essentials certification – which is simpler, cheaper and quicker to obtain than the much more complex ISO 27001. The handful of respondents (3%) who have PCI DSS certificates is perhaps not surprising: while recommended by many card processing service providers, PCI DSS is often not mandated and so companies are under no obligation to incur the cost of becoming certified.

37% of organisations have no certification, and slightly fewer (32%) say that they work to a standard but don't hold a formal certification. In our experience the level of conformance in the latter group varies significantly: while some organisations have rigorous security regimes and may be in good shape were they to undergo a formal audit, many would fall well short.

Recommendations

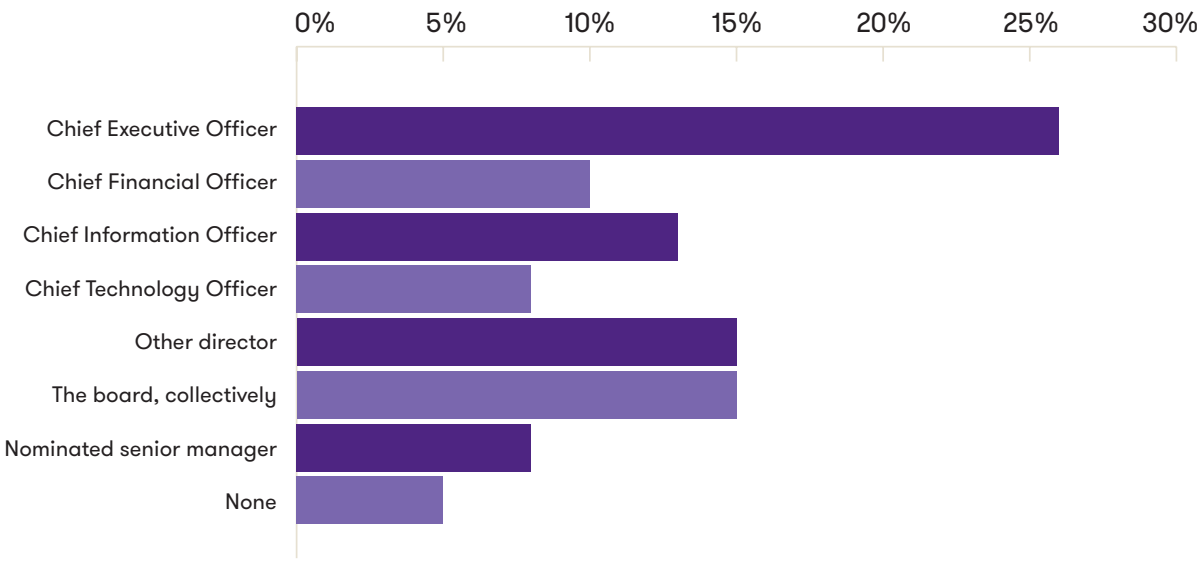
Get Cyber Essentials certification. It's a brilliant set of simple steps that will protect you against the vast majority of security breaches, and it's inexpensive and straightforward to do.

Consider ISO 27001 if you're a medium or large enterprise. Holding an ISO 27001 certificate is one of the most effective ways to convince your suppliers and customers that your security regime is robust and is operating effectively: more importantly, implementing the controls and monitoring required by ISO 27001 will inevitably make your organisation more efficient and more secure, will improve your ability to see how the company works, and will help you improve over time.

Don't be "compliant" – be certified. If an organisation says it complies with a particular standard but hasn't gone all the way to the independent audit, ask yourself why. There are many, many companies that claim to be ISO 27001 "compliant", for instance, but which wouldn't stand a chance of passing an independent audit. Don't claim to be compliant with something – take the extra step and become certified.

Detailed results

Which member of your leadership team has overall responsibility for information security?



Results

This is one of the most varied categories in terms of responses, with the most common port of call for security responsibility being the CEO (**26%**). The CIO (**13%**) and CTO (**8%**) have their fair share of responsibility: although there is a school of thought that prefers security to live outside the IT and technical teams in the interests of independence (e.g. in the **10%** of cases where the CFO takes it on, or the **15%** where it's down to another director), CIO/CTO responsibility clearly works for many. Collective board responsibility scored **15%**, and in an intriguing **5%** of cases there is nobody considered responsible for information security.

Recommendations

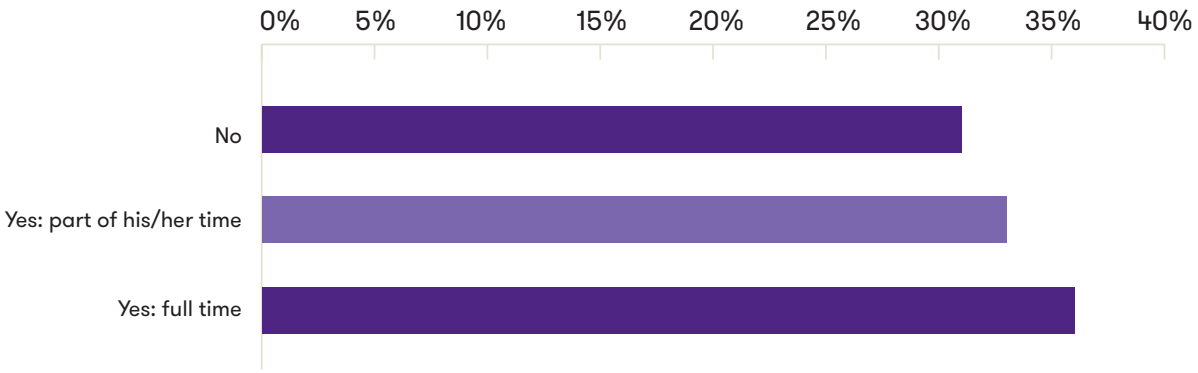
Have a specific person responsible for information security. They should be the "go to" person if someone has a security question, or someone identifies suspicious activity or a potential threat.

Remind the board that they are ultimately accountable for security: even if you have an individual responsible for collating security data and disseminating information, it's the board that decide how to deal with the risks that the responsible person presents to them, and it's the board who can redirect funds to deal with significant risks (or, conversely, can agree that a risk can be tolerated and decide to live with it).

Consider **whether the CTO or CIO is the right person** to be responsible: it works for many businesses, but there's potential benefit in having the oversight of security in a different division from the one that's responsible for implementing secure systems.

Detailed results

Aside from the leadership responsibility, do you have at least one member of staff specifically responsible for information security?



Results

This question resulted in a roughly even split: **36%** of respondents have a specific, full-time individual responsible for information security, with a part-time nominated individual only slightly less common (**33%**). The remaining **31%** – almost a third – have nobody nominated to look after information security, which we find surprising given the prominence and importance of information security to both individuals and businesses.

Recommendations

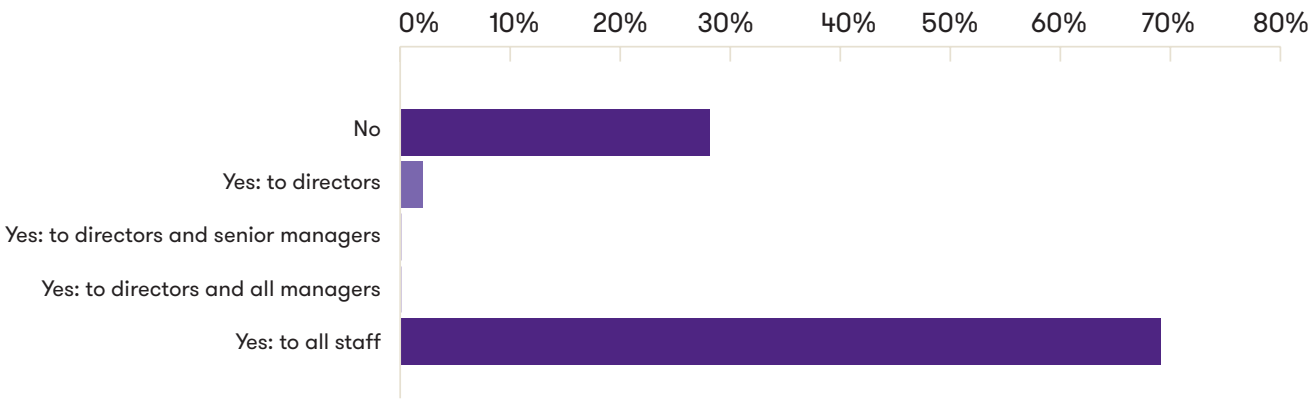
Have a specific person responsible for information security, even if it's only on a part-time basis.

Provide suitable training and other resources so that the responsible person has an acceptable level of expertise and is able to keep up with trends in information security.

Give senior management backing to the responsible person: it's a lonely role if the security co-ordinator isn't seen to have backing from the top of the company.

Detailed results

Do you provide information security training at least annually to your staff?



Results

This is the most reassuring question of all, with over two thirds (69%) of companies providing information security training to all their people. Sadly, celebrations aren't yet due thanks to the 28% who aren't giving regular training to everyone. The 3% who train their directors are heading in the right direction – after all, the board are ultimately accountable for protecting the organisation's sensitive data.

Recommendations

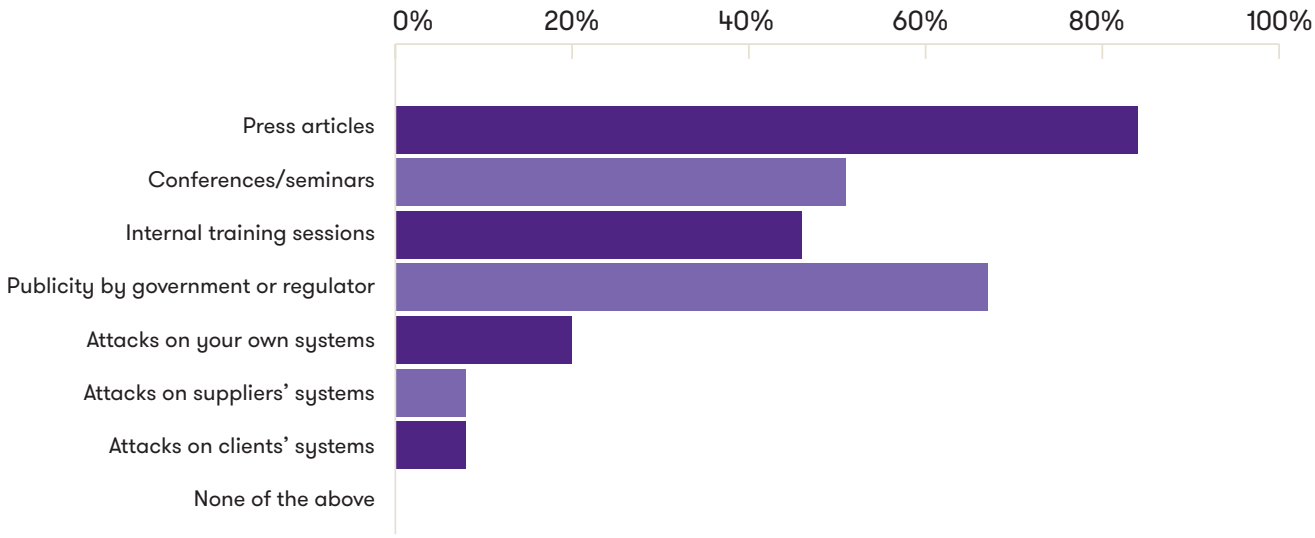
Give regular mandatory training to all staff, even if it's only some basic computer-based training. Try to have a structured campaign, though: do face-to-face presentations at least a couple of times a year with email or computer-based elements in between.

Communicate real examples of security issues you've had, as long as you're not breaking confidences or embarrassing individuals. Staff relate best to real-life security problems in your own business – it brings home the fact that information security relates directly to them.

Have an annual seminar for the board/executives: get a top-level security specialist to work with them and help them understand the particular risks and responsibilities that exist at senior level.

Detailed results

Which of the following have raised your awareness of information security risks in the last year?



Results

This question invited respondents to tick all of the ways in which they find out about information security: the runaway leader is press articles, with **85%**. Information from the public sector is also a source of information for about two thirds of respondents – **67%** – which implies that the public funds being spent on raising awareness are not going to waste. Half (**51%**) of the replies cited conferences and seminars as a means of finding out about security, and at **46%** almost half learn thanks to internal training.

Bitter experience is, however, a significant way of learning about security – **21%** learned the hard way from attacks on their own systems, with a total of **16%** finding out through attacks on the systems of their clients (**8%**) or suppliers (**8%**).

Recommendations

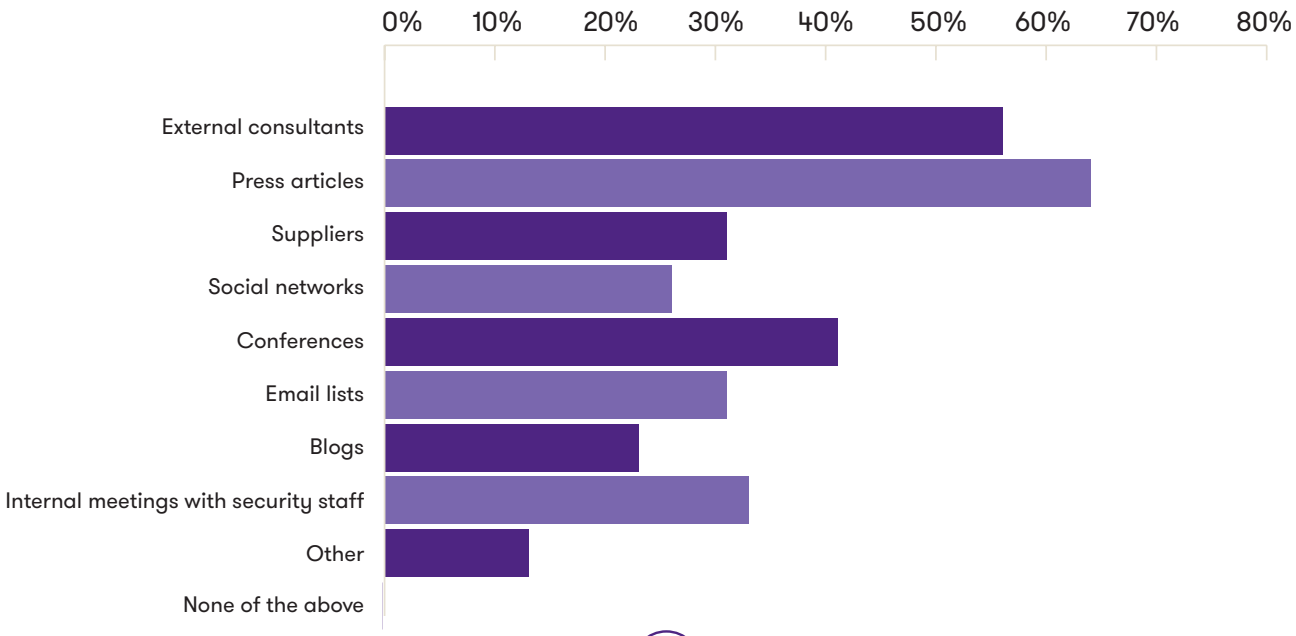
Use the free resources available to you: the IT press is a fantastic source of timely, relevant information on security issues; social media (particularly LinkedIn), blogs and mailing lists supplement the press superbly too.

Learn from attacks: when, metaphorically speaking, you've "put out the fire" of an attack, do a "lessons learned" exercise, be honest about what went wrong, and take the necessary actions to make a recurrence less likely.

Attend conferences and seminars, but do so sparingly. You probably have a dozen options each month, and you can't do them all: be pragmatic and attend the one or two a month that you think will have the most value.

Detailed results

How do you proactively stay informed of new security threats?



Results

At **64%**, the press is again a popular choice for proactive reading on security threats, though only slightly fewer (**56%**) use external consultants to further their knowledge and **31%** take advice from suppliers. A little under half (**41%**) attend conferences, with a fair chunk of the audience reading electronic sources such as social media (**26%**), email lists (**31%**) and blogs (**23%**).

Internal meetings also had a significant part to play, with **33%** of those who replied citing them as one of their ways of finding security information proactively.

Recommendations

The recommendations from the previous questions apply here too, particularly with regard to keeping an eye on the press and the conference circuit. In addition:

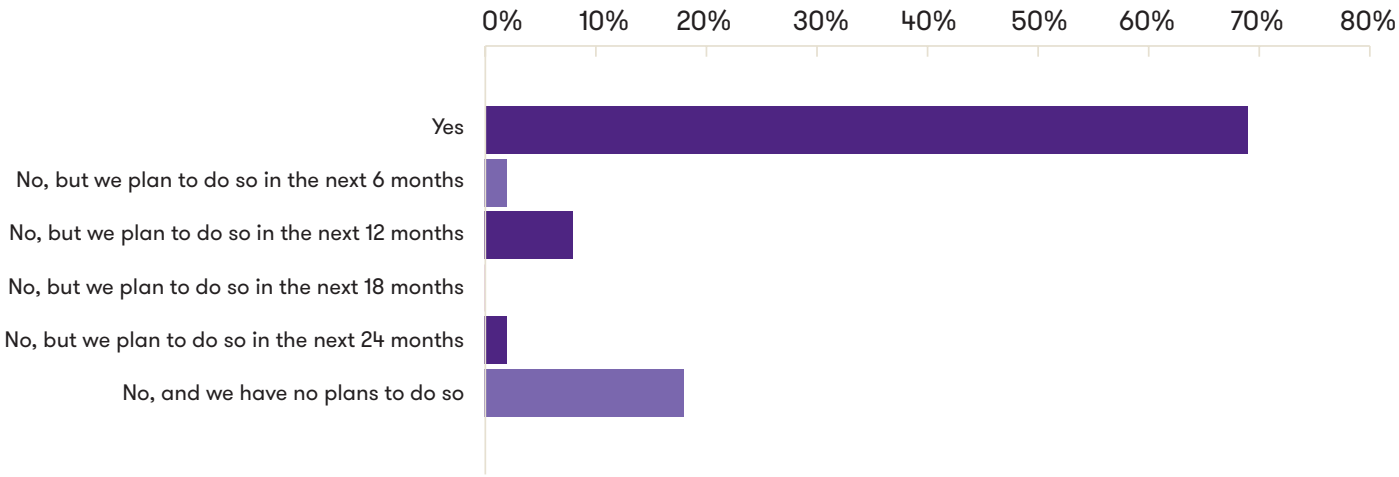
Use your supplier relationships. Your suppliers should also have their own security regimes, so include security as one of the agenda items on your regular service reviews. They should be keen to please you in order to retain your business, and giving you regular updates will cost them next to nothing and will bring value to you and to the relationship.

Use external specialist consultants. Many will happily engage on a retainer basis, to provide a few hours' advice per month when you come across something that you don't understand or don't have the time or resource to look into. It's an inexpensive way to access specialist knowledge and extra resource when you need it.

Talk internally about security. By meeting with your information security specialist or team every month, or even once a quarter, the divisions of the company will be better informed about information security in general and current threats in particular, and will be better placed to operate securely.

Detailed results

Have you carried out a structured assessment of your cyber security in the last 24 months?



Results

Over two thirds (69%) have conducted a formal review of their information security in the last two years. Of those who haven't, 11% intend to do so in the next year and a further handful (3%) in the next two. Given the prominence of security threats, the 18% who have no intention of conducting an assessment are a cause for concern.

Recommendations

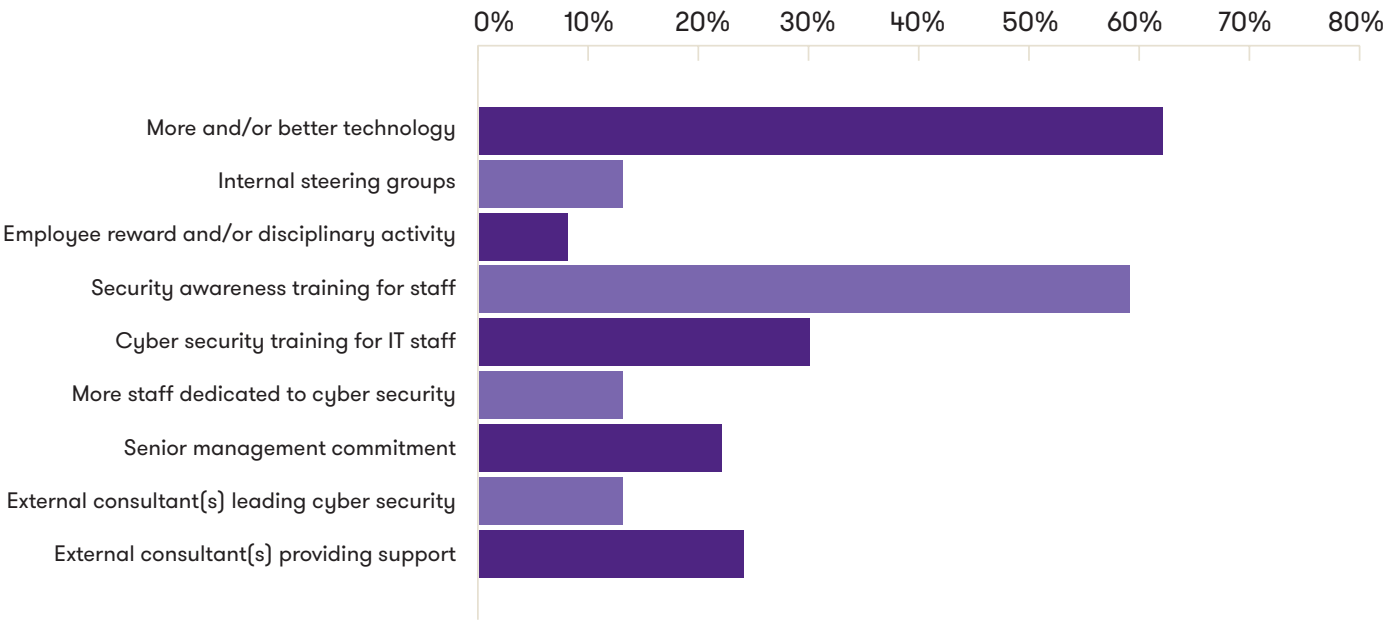
Assess your security at least annually, preferably more frequently and preferably by using an independent assessor.

Act on the results of the assessments: for each of the risks thrown up by the assessment, agree a plan and act upon it.

Assess internal security as well as external security. Ask yourself "what if". If server X were compromised, what other systems could the attacker access? If user X's login ID were compromised by ransomware, what percentage of the company's file server contents could it encrypt? Always assume that you could be hacked, and ensure that you consider the damage that could be done when this happens.

Detailed results

Which of the following do you intend to implement in the next 12 months to maintain or improve your cyber security?



Results

Technology plays a big part in the plans of almost two thirds (62%) of respondents. Almost as many (59%) plan security awareness training for their people, with 30% intending to give their IT staff specific cyber training. External consultants have a part in the plans of 38% of respondents: 14% will have them running the cyber function, with 24% intending to use them to support the internal cyber security efforts.

Senior management commitment plays a part for a fifth (22%) of people, and 14% want to increase the number of staff that have a focus on security; a similar number (14% again) think steering groups are a useful way forward. Bringing up the rear on just 8% is the use of reward or discipline to further the cause of security.

Recommendations

We've already covered training in previous questions, so we won't repeat ourselves.

Senior management commitment is essential to security. If staff see that the board/executive are committed to security as part of the company's strategy, they are more likely to focus on it.

Use appropriate technology: don't roll out a vast range of new security systems if you don't have the expertise to use them or the resource to monitor them. The worst sin in information security is to have a system that contains all the data you needed to identify a vulnerability or a breach, but to not look at the data because nobody had time to do so.

Keep your technology up to date. Any system that was secure on day one will probably not be secure on day 301: without regular updates your systems will be susceptible to the vulnerabilities that cyber criminals – and the system vendors – discover over time. It's better to have a small number of systems that are rigorously maintained than a vast collection that's full of old operating software with security bugs.

Detailed results

If you were to outsource some or all of your cyber security capability, what would you want them to do and how would you like the relationship to function?

Results

Of the variety of replies we had to this question, there were three common themes. We picked just a handful from the various responses to this question.

We're fine (at least for now)

Some companies were content with their current situation. One respondent said:

At the moment we are happy to stay as we are, but [may consider outsourcing] in due course

… while another stated that outsourcing was simply:

Not under consideration

Outsourced independent review

Some respondents are considering outsourcing a one-off review, one example being:

We would want a firm to conduct an initial review to address areas of weakness and provide solutions

Outsourced ongoing function

This was a popular area, and responses fell into two camps. One was to outsource a particular function to a third party:

Legislative and compliance monitoring via consultancy

… while the other was to engage an outside supplier to supplement internal talent:

Provide independent threat management consultancy services to complement internal processes and teams

Conclusions

We could make pages of observations based on the findings of our survey – but of all the actions you could take having read this report, these are the five that matter most and will bring the greatest benefit.

Awareness training

69% of respondents said they train their staff, yet 67% said that if they have a security breach in the next year, it'll probably be because of an accidental error by a member of staff. Although one can of course never prevent all staff errors, these results suggest that there is room for improvement in the training that's being given.

Use of technology

The above point should also be borne in mind by the 62% of respondents who said they would use more and/or better technology over the next 12 months to improve security. Just as training won't fix all security problems, neither will technology – but technology can help. For example, something as simple as disabling "autocomplete" for the recipient address in an email application will stop thousands of breaches each year (most of us have, after all, sent email to the wrong person because Outlook guessed the address and we didn't notice the mistake). And the introduction of secure file sharing instead of using email for sensitive data will give much better control over the data that's being shared with others.

Cyber Essentials

Despite being a great model that provides excellent protection for just a modest effort, only a tiny minority presently have it in the Channel Islands. We absolutely recommend getting your systems up to the necessary standard, and then applying for CE certification. Additionally, the UK government already mandates CE for much of its procurement activity, and we expect the governments of the Channel Islands to follow suit.

Central point of contact

If you have a central point of reporting for security concerns, you stand a much greater chance of identifying common problems: if you don't have one, people simply won't know who to contact if they have a concern. It doesn't necessarily have to be a full-time job – as we've seen, almost half of those who have a central contact do so on a part-time basis – because simply having a specified contact is far better than having none at all.

External support

Some organisations can afford and justify large teams of experienced in-house security professionals who need no external assistance – but these organisations are in the minority. 38% of respondents intend to use third party support in the next year to bolster their internal capabilities, which makes sense because you can select outside help in any area of expertise you need, and pay for it only when you require it.

grantthorntonci.com