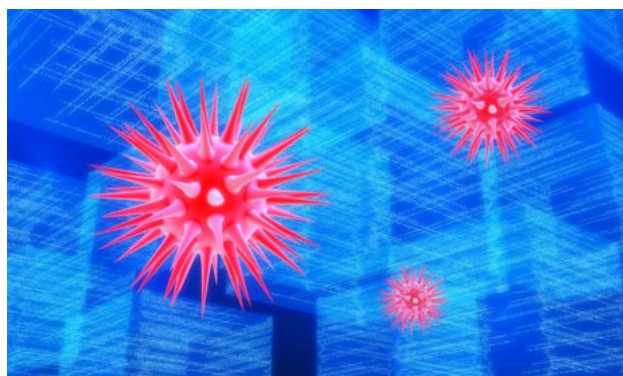


Live discussion: Should local government be worried about cyber security?

Join our panel from 12pm on Wednesday to discuss hacking, viruses and data security in our online debate. Post your comments now or tweet us: [@GdnLocalGov](https://twitter.com/GdnLocalGov)

Kate McCann

Guardian Professional, Tuesday 29 November 2011 16:34 GMT



How can local government protect itself from computer viruses? Photograph: Sebastian Kaulitzki / Alamy/Alamy

When we tweeted about cyber security in local government last week some of the responses we received were surprising. They ranged from bewildered questions to claims that local government isn't interested in cyber security, and even some confusion over what the phrase actually means.

But many of you are very interested in the issue and keen to learn more. Cyber security often refers to attempts to combat cyber crime, including viruses and hacking, but can also include data protection and network safety – all essential elements of running a successful and safe local authority.

You can read more about the UK cybersecurity [plan here](#).

With local government embracing cloud computing and other shared digital services, councils will have to be on top of network security, especially when they guard sensitive data about us all. So what threats could local authorities face, and how can they protect themselves for the future?

Join our panel from 12pm on Wednesday. Post your comments and questions now, or tweet us at [@GdnLocalGov](https://twitter.com/GdnLocalGov).

Panel:

Andrew Miller leads on government information security services at [PricewaterhouseCoopers \(PwC\)](#). Prior to joining PwC, Andrew worked for Fujitsu Defence and Security, where he was responsible for the transformation of the company's security services portfolio.

Tara Savage is senior marketing manager at [BT Global Services](#). Tara has been responsible for a number of strategic security campaigns as well as co-ordinating a

series of global training programmes. Tara currently co-ordinates BT's work with external security market analysts, ensuring that BT is recognised as a leading security provider.

Richard Carty is the commercial director of [Netshield](#), which specialises in the delivery of complete IT services. Richard has more than 30 years experience in IT and specialises in business continuity planning and managed hosting services.

Katrina Day is an associate at [Coffin Mew LLP](#) and specialises in providing data protection advice, primarily to the social housing sector.

Mike Gillespie is managing director of [Advent IM Ltd](#). Advent IM provides bespoke services to organisations requiring information security.

Karl Smith is head of cyber security assurance services at [BT Global Services](#). Karl is responsible for the delivery of the company's cyber security portfolio, including Cyber Defence Quickstart and CHECK and CREST, which helps protect against hacking.

This live discussion is designed and managed by the Guardian local government network to a brief agreed with BT, sponsor of our [digital innovation hub](#).

Ads by Google

[KPI Whitepaper - Download](#)

Public Sector Whitepaper. Produce meaningful KPI's.

www.sas.com/uk/public_sector

[Phish Your Employees](#)

PhishMe- The Leading User Awareness Education Service

www.PhishMe.com

[5* SIEM Product Review](#)

See Why SC Labs Recommends Our Five Star SIEM Product. Free Download.

www.logrhythm.com

Comments in chronological order (Total 63 comments)

 Staff

 Contributor





[KateEMcCann](#)

30 November 2011 11:00AM

Morning all, some great articles on the very topic can be found on Guardian's Government Computing site [here](#).

Feel free to post your own links here too ahead of the discussion today.

Recommend? (0)

Responses (0)

[Report abuse](#)

 Clip

| [Link](#)





[KateEMcCann](#)

30 November 2011 12:00PM

Afternoon everyone and welcome to this live discussion about cyber security and networks.

While the panel introduce themselves it would be great to have some questions if someone would like to start us off. I would be interested in finding out more about what local government's role is currently in protecting networks and data, and what we might expect it to be in the next 5-10 years.

Thanks

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[MikeGillespie](#)

30 November 2011 12:04PM

Hi, I'm Mike Gillespie of Advent IM Ltd. We are one of the UK's leading independent holistic security specialists. Security is not just about product ... its more about policy, procedure and premises ... and educating staff on best practice. Thats why we help public sector customers implement best practice standards.

Recommend? (0)

Responses (1)

[Report abuse](#)

[Clip](#)

| [Link](#)



[karlsmithbt](#)

30 November 2011 12:06PM

hello everyone my name is Karl Smith i head Cyber Security Services for BT Global services

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[Tarasavage](#)

30 November 2011 12:07PM

Hi, I'm Tara Savage from the Business Continuity Security & Governance team in BT - interested in finding out from those participating what their key challenges have been over the past 6 months - do they feel that they're fighting fires or are they able to be at all proactive when it comes to Security?

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[KatrinaDay](#)

30 November 2011 12:08PM

Hello I am Katrina Day a solicitor with Coffin Mew LLP, specialising in data protection advice. I agree with Mike's comment as in my experience a lot of data security issues arise from human error and not being fully educated about how best to use the technology and products available.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)

C



[AndrewMillerPwC](#)

30 November 2011 12:09PM

Hello there, I'm Andrew Miller - I run the public sector Information and Cyber security business for PwC.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)

C



[AndrewMillerPwC](#)

30 November 2011 12:11PM

Local government are the devolved custodians for constituents information. That's a significant amount of important information that needs to be looked after. Quite often its the simple things that need to be done consistently which gain the most benefit in terms of defence against the Cyber threat. Patching of systems, up-to-date antivirus and user awareness are all core elements of an effective Information Security plan. If executed appropriately give a stable base to begin increasing an organisations Cyber Situational Awareness.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[jamesdoxon](#)

30 November 2011 12:11PM

Panelists, what is your view on the current ability of local government to respond to the latest security threats, vulnerabilities and most importantly realised attacks on their systems, and where do you think they will be in three years time?

Do you think we are all working from the same concept of what "cyber security" actually is, or does the use of that term lead to the confusion mentioned in the introduction above.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)

C



[karlsmithbt](#)

30 November 2011 12:15PM

Within BT we provide a suit of Cyber Security services which are a combination of adaptive technology and business risk frameworks, in speaking to a lot of customers I find that one of the key issues is understand which are the key assets or crown jewels Of the organisations.

Q:

What approaches do you take from an organizational standpoint to help understand your Organisations security posture, and also prioritize risk?

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[MikeGillespie](#)

30 November 2011 12:16PM

Hi James. I doubt very much we are all working to the same concept of cyber security. At the top government level it has terrorist implications and is really where the phrase started in earnest post 9/11. Whereas to local government and indeed the private sector generally its probably more about the day to day protection of your network from DoS and hacking.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[RichardCarty](#)

30 November 2011 12:18PM

Hi Richard Carty of Netshield Limited here, I believe one of the biggest issues in all of the comment areas so far is getting users to understand the size of the threat and how vulnerable they all are, rather than thinking IT security breaches are something that happen to "somebody else" they need to be educated, that at some point it will happen to them!

Recommend? (0)

Responses (1)

[Report abuse](#)

[Clip](#)

| [Link](#)



[MikeGillespie](#)

30 November 2011 12:18PM

In response to your first question, in my experience Local Gov is not prepared to handle security threats across the board. In July it was revealed that 3/5 of Englands largest Councils were failing to comply with the GCSX/GSi GoCo requirements for protective monotoring. Although central gov has to implement such controls, this a new concept to local gov ... but one which is starting to catch on.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[AndrewMillerPwC](#)

30 November 2011 12:19PM

Adding to Karl's question, are the business roles within local government ready to make decisions on the impacts of cyber incidents. With increasingly little time to respond to events what business support and communication strategies are in place to deal with an evolving scenario.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)

C



[MikeGillespie](#)

30 November 2011 12:20PM

Absolutely Richard. You can't protect something you don't understand - which is where understanding threat and risk comes in - and you can't get that from a box with flashing lights.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)

C



[Tarasavage](#)

30 November 2011 12:21PM

Usually when we talk about cybersecurity we focus on the negative impact of an attack on reputation, on customer relationships, and on remediation. But by then, the damage has usually already been done; reactive strategies mean that the network is already compromised, that data is already lost, and reputations in tatters.

I think local government is still on the reactive side of the fence when it comes to current threats.

Getting the headroom to be proactive is fundamental - but that's easier said than done, especially with limited resources. I agree with Andrew that getting the basic/simple things right is vital but then are there other areas where local government could look to be proactive - looking at threat monitoring and denial of service mitigation perhaps.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)

C



[karlsmithbt](#)

30 November 2011 12:22PM

James & Mike indeed i think everyone's definition of "Cyber Security" differs slightly ranging as suggested from the full spectrum of threats to specific issues such as "Hactivist" threats, DDOS attacks, and blended threats such as malware and bonnets

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)

C



[AndrewMillerPwC](#)

30 November 2011 12:23PM

Response to [RichardCarty](#), 30 November 2011 12:18PM

With some of the emerging threats actually hiding their extraction of information it's quite possible that it's already happening to them, they just aren't looking/noticing it's happening

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)

C



[RichardCarty](#)

30 November 2011 12:24PM

Organisations like mine (Netshield) and others can provide technical solutions and services to technical threats but the bulk of attacks/penetrations/breaches are of a non technical or even human nature!

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)

C



[RichardCarty](#)

30 November 2011 12:27PM

Indeed Andrew organisations need to take the human aspect as seriously if not more so, than the technically accomplished hacker

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)

C



[AndrewMillerPwC](#)

30 November 2011 12:27PM

Once the basic's of patching etc. are in place the Local Gov organisations should look to achieve basic Situational Awareness, as previously stated above, many don't have this insight into "what's going on" on their systems. But this in itself needs to be blended with an organisational structure that is able to deal with the Management Information this creates. Its all well and good having an alert appear on a screen somewhere, it needs action and I don't think this structure exists in many cases at the moment.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)

C



[AndrewMillerPwC](#)

30 November 2011 12:31PM

It's supprising how the security culture of an organisation can mitigate many of the inadvertant or accidental cyber incidents. The two fines the ICO gave local councils recently around Personal Information losses were human in nature for instance.

<http://www.guardian.co.uk/government-computing-network/2011/nov/28/ico-fines-worcestershire-north-somerset-data-breaches>

Recommend? (0)

Responses (1)

[Report abuse](#)

[Clip](#)

| [Link](#)

C



[karlsmithbt](#)

30 November 2011 12:32PM

As Richard has stated adversaries and hackers will go after the "human Layer" and will exploit social networking and other avenues to glean information that benefits a Blended Attack path. User education and awareness programs therefore must also form part of a good defensive "Cyber Security" strategy for public sector organisations

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[MikeGillespie](#)

30 November 2011 12:33PM

Yes and indeed the council worker that left documents and a computer in a vacated office last week didn't make a malicious attack on its employer ... but a genuine mistake. Its the old adage of 2/3 of breaches come from within.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[MikeGillespie](#)

30 November 2011 12:35PM

Yes but back to James - our first postee - what is cyber security? and where does cyber security end and data security start. The Government needs to define this clearly and how they expect all levels of Government to play their part.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[RichardCarty](#)

30 November 2011 12:35PM

We work with a number of legal organisations to provide e-fraud seminars, to demonstrate live in front of their eyes, how easy it is to be hacked personally and technically, which always has a dramatic effect on the audiences we present to at our seminars, more of this sort of awareness needs to be generated in Local Government arenas, to get the message out!

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[KatrinaDay](#)

30 November 2011 12:36PM

Response to [AndrewMillerPwC](#), 30 November 2011 12:31PM

Agreed Andrew, all of the major fines issued by the Information Commissioner to Local Authorities have elements of human error (such as sending an email to the wrong contact group), where education would potentially have helped to prevent the problem. There does also seem to be a lack of using more basic technology such as encryption and password protection which is worrying when we are looking at much more technical security breaches here.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[AndrewMillerPwC](#)

30 November 2011 12:36PM

Here at PwC we have taken input from our global network of Security Professionals to produce the business leadership point of view on Cyber Security. It helps frame the non technical elements for business leaders and would be as applicable to leadership in local councils as multinationals.

<http://www.pwc.co.uk/eng/publications/delusions-of-safety-cyber-savvy-ceo.html>

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[MikeGillespie](#)

30 November 2011 12:39PM

Katrina is absolutely right. In our experience technologies such as encryption and password usage are in place but many Council employees don't understand why the controls are there and how to use them properly. Encryption is a prime example as staff believe that when they have an encrypted laptop it must always be encrypted ... when in actual fact its only encrypted when its turned off. Education education education

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[KateEMcCann](#)

30 November 2011 12:40PM

Hi all, some of you may have noticed that you can now respond directly to posts by clicking on the 'Respond to this' button next to each comment.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[HannahFearn](#)

30 November 2011 12:43PM

My question for the panel is: are local authorities likely to be candidates for a cyber attack during major events? Could, for example, the London boroughs face deliberate digital disruption during the 2012 Olympic Games?

And if so, how can councils realistically prepare for this now during a period of intense and painful cost cutting?

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[ADVENT](#) [in](#) [MikeGillespie](#)

30 November 2011 12:51PM

Hi Hannah. A question I'm sure that worries many local authorities. The answer is ... we don't know. But like any threat it has to be considered as part of the authorities risk assessment process. Personally I think attacks are more likely to be aimed at Central Gov but we don't know what we don't know! Regular external penetration tests will provide assurance and I think Andrew mentioned the importance of patching earlier. As key players in the compliance with the Civil Contingencies Act you will have processes in place to ensure continuation of critical services. My starter for 10 would be carry out that pen test and take it from there,

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[ADVENT](#) [in](#) [MikeGillespie](#)

30 November 2011 12:52PM

Everyone is a candidate for a cyber attack and much of it is untargetted and indiscriminate.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[KateEMcCann](#)

30 November 2011 12:55PM

All, is cyber security and protection expensive for local government?

Recommend? (0)

Responses (1)

[Report abuse](#)

[Clip](#)

| [Link](#)



[JennyPurt](#)

30 November 2011 12:55PM

Hi All,

I'd be interested to know more about what problems cloud technology could present for local government?

Thanks,

Jenny

Recommend? (0)

Responses (1)

[Report abuse](#)

[Clip](#)

| [Link](#)



[JessicaF](#)

30 November 2011 12:57PM

Hi, I'm interested to hear more on people's views about any potential threats or problems cloud technology may bring to local government? Surely such technologies increase the amount of risks hugely? How are local authorities prepared to deal with such potential risks?

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[SadeLaja](#)

30 November 2011 12:58PM

Response to [MikeGillespie](#), 30 November 2011 12:04PM

@MikeGillespie I write for the Guardian Government Computing Network, and I was quite interested in your point about security not just being about the product, but also about policy, procedure and educating staff.

I just wondered, in practice how easy is it to educate staff about security threats, and what could local government organisations do to further aid this process?

Recommend? (0)

Responses (1)

[Report abuse](#)

[Clip](#)

| [Link](#)



[AndrewMillerPwC](#)

30 November 2011 12:58PM

As Mike suggested, there will have already been risk assessments taking place at various levels looking at this problem. I suspect the main areas at risk have been working on this problem for a while now. I would anticipate for Local Gov one area they are seriously considering is how to effectively work during next year. Remote working is a popular option for many with organisations making investments in this area, penetration tests and capacity tests will be important when relying on this type of solution as a main method of doing business for extended periods, especially when it may not be the norm at the moment in such high volumes of telecommuters.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[MikeGillespie](#)

30 November 2011 1:04PM

Response to [JennyPurt](#), 30 November 2011 12:55PM

Hi Jenny. Security is the biggest problem but cloud computing whilst a great concept is not as simple as it sounds and needs a great deal of thought. Firstly what are you going to use it for an why, what type of data will be held there, who will need to access it. The decision must be risk assessed and controlled. If there are off-shoring implications as well eg you have datacentres in India, thats a whole different ball game. Also are you having your own private cloud which is essential the next gen of intranet. Is that cloud in a public cloud so do you actually know where its going ie have you set any endpoint restrictions.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[benjoda](#)

30 November 2011 1:05PM

I work with very advanced tools to harvest data and user profiles on the web. I always work ethically but if I was to point those tools at any of you domains now, how confident are any of you that you would be secure and are you happy for me to test your domains right now ?

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[karlsmithbt](#)

30 November 2011 1:07PM

within BT we are contributing to the Olympic effort our public facing site is here:

<http://www.btplc.com/btlondon2012/ataglance/>

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[MikeGillespie](#)

30 November 2011 1:09PM

Response to [SadeLaja, 30 November 2011 12:58PM](#)

Hi Sade. Awareness training does not have to be onerous or difficult. All staff should be trained on induction and receive regular training updates throughout their employment. Security is everyones responsibility. However, there obviously issues with the number of staff employed by Council's and how do you get to them all. This can be address through policy software which requires users to accept policy updates and changes when logging onto the network, training can be provided on a need to know basis based on job role. There is also CBT training/on-line training which can help reach the masses and requires an exam at the end. I know a Council we work with also sends regular information security newsletters to staff. For reactive responses, there are bulletin boards, email broadcasts, intranet notices that can be used to reach people quickly.

Recommend? (0)

Responses (1)

[Report abuse](#)

[Clip](#)

| [Link](#)





[AndrewMillerPwC](#)

30 November 2011 1:09PM

In response to Jenny and Jessica, adoption cloud needs to be a risk based business case. The benefits can be significant in terms of technology costs and flexibility however it comes at a price. Depending on what type of Cloud service you buy-into, your information could be in the UK or more likely in a string of off-shored data-centres. With current providers, again depending on what service you purchase, most will use their own practices and policies to protect your information, which may or may not be equivalent to your expectations.

As you can tell, not all cloud providers are the same, commodity players will offer minimal generic protection where as neiche or high end providers will be able to meet more of your security expectations. It's best to take advice which allows your particular situation to be taken into account.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[benjoda](#)

30 November 2011 1:14PM

Is that a re-sounding NO to the idea of a live, ethical hack while this discussion is progressing then ?

Fair enough - but I thought it would add some spice....

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[AndrewMillerPwC](#)

30 November 2011 1:14PM

Response to [MikeGillespie](#), 30 November 2011 1:09PM

Building on Mike's point, these tools have a value in scale, we often use these tools to reach employees in global organisations. Local Councils could group together around education and awareness services and gain the benefit in development and roll-out costs. Through this effort the cost of some of the more niche elements can be covered as it's not getting generated time after time. This can easily include specialist variations in other languages and for the visually impaired.

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[AndrewMillerPwC](#)

30 November 2011 1:18PM

Further to the Cloud question here is a PwC paper on Secure Cloud

http://www.pwc.co.uk/eng/publications/cloud_computing.html

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[jamesdoxon](#)

30 November 2011 1:20PM

Response to [KateEMcCann, 30 November 2011 12:55PM](#)

Kate, taking basic security and protection measures need not be overly expensive - especially in comparison to the potential costs of inaction. What can be difficult and expensive for the public sector is finding and retaining skilled information security practitioners.

Recommend? (0)

Responses (1)

[Report abuse](#)

[Clip](#)

| [Link](#)



[AndrewMillerPwC](#)

30 November 2011 1:23PM

In reference to Kate's question about Cyber costs, anyone can use the 2012 PwC Global State of Information Security Survey portal to give them some indication on spend. Just click on Explore Surey Data to run online queries.

<http://www.pwc.com/gx/en/information-security-survey/index.jhtml>

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[MikeGillespie](#)

30 November 2011 1:25PM

James you make a very valid point, which is often why we have found ourselves supplementing and complementing skills within the public sector.

<http://www.advent-im.co.uk/mysecuritymanager.aspx>

Recommend? (0)

Responses (0)

[Report abuse](#)

[Clip](#)

| [Link](#)



[HannahFearn](#)

30 November 2011 1:29PM

Some really interesting comments and advice shared here today. Does the use of social media and networked communication put local government at any greater risk? It's obviously an important part of the way it will work in future, but are there risks as well as benefits when it comes to online security?

Recommend? (0)

Responses (2)

[Report abuse](#)

[Clip](#)

| [Link](#)

Comments on this page are now closed.

On this site

[About us](#)

[Advisory Panel](#)

[All today's stories](#)

[A-Z of this site](#)

[Become a member](#)

[Blog](#)

[Twitter](#)

[Big society](#)

[Commissioning](#)

[From the front line](#)

More topics

[Organisational development](#)

[Outsourcing](#)

[Professional development](#)

[Social care](#)

More topics

[Social work](#)

[Training](#)

[Workforce development](#)

Contributors

© 2011 Guardian News and Media Limited or its affiliated companies. All rights reserved.