

Cyber Security in Local Government Pre-Discovery

Local Digital Collaboration Unit Cyber Team

13 May 2020



Ministry of Housing,
Communities &
Local Government

Contents

[Executive summary](#)

[Why we are doing this work](#)

[Pre-discovery goal](#)

[What we did](#)

[What we learned](#)

[Protecting against a cyber attack](#)

[Responding to an incident](#)

[Recovering from an incident](#)

[Ransomware survey results](#)

[Hypotheses](#)

[Recommendations for further work](#)

[Gaps and limitations](#)

[Appendices](#)

Executive summary

Local and central government are repeatedly having to financially support recovery from malicious cyber attacks, costing millions of pounds and impacting the lives of citizens.

An increasing use of technology brings a parallel, greater need to maintain secure local government services for citizens by:

- mitigating exposure to risk
- protecting from the threat of attack
- responding appropriately
- recovering quickly

This pre-discovery is motivated by a need to understand how central government can reduce risk and optimise spending in support of, and collaboration with, local authorities. It is the first step in understanding a complex and uncertain space.

Our aim was to identify themes and areas that might offer opportunities.

Investigation and analysis took the form of both qualitative and quantitative research.

We analysed 173 (48%) responses from English councils to survey questions generated around NCSC guidance from the 'Mitigating Malware and Ransomware Attacks' publication.

We interviewed users who are instrumental in maintaining cyber security at local authorities, in order to understand their perceptions and challenges.

We spoke to organisations engaged in supporting local authorities in this space.

From our research we uncovered nine interrelated themes.



We found and heard that:

- cyber security is often viewed as a technical issue, rather than a business issue, and is not seen as being everyone's responsibility
- there is no one single solution that could solve cyber risk at local authorities as issues vary in size, severity and context
- there is evidence of both good and bad practice across local authorities
- cyber security is made up of many interrelated aspects
- a potentially overwhelming amount of guidance paradoxically often leads to a lack of clarity and confusion

Given more time and scope, we would have liked to:

- gain a deeper understanding of current cyber security standards including technical, assurance and governance
- achieve a greater understanding of the context behind the quantitative ransomware survey responses
- investigate new themes as they emerge
- speak to more users and stakeholders from a variety of roles
- conduct more in-person research enabling greater empathy and understanding due to Covid-19
- gain a greater understanding of private sector service provision, tools and training

We consulted senior stakeholders working in cyber security to gain feedback on the nine hypotheses generated from our findings. There was strong consensus that three areas in particular have a greater potential to help support local authorities with cyber security:

Vulnerability to cyber attacks would be reduced if local authorities build, plan and maintain services in a secure manner.

Cyber security risk would decrease at local authorities if they subscribed to clear standards, expectations and goals.

Cyber security risk would be reduced if behaviours, ownership and responsibility for cyber health at local authorities were improved.

We will now look to:

- define the problem space around the three prioritised themes
- quantify the value of increasing cyber security across local authorities
- understand the capabilities, disablers and enablers related to the three prioritised hypotheses

The remaining themes, while not a priority, still have the potential to contribute to our goals.

**Why we are doing this
work**

Understanding the impact of cyber security

Q1. How long did Copeland Borough Council take to recover from a severe cyber attack in August 2017 and at what cost?

2.5 years and £2.5M excluding staff support cost such as counselling

Q2. What phrase did Copeland's Borough Council Chief Executive use to describe their recovery effort?

“Beyond Challenging...”

Q3. How many attempted breaches of UK local authorities occur every minute according to the Big Brother Watch report, released February 2018?

37 attempted breachers per minute

Pre-discovery goals

Pre-discovery goals

Our goal was to research, identify and understand the current landscape of threats, challenges and current capabilities, in the area of cyber security, across local authorities.

We set out to:

- understand threats and vulnerabilities
- understand the landscape and those operating within it
- understand the challenges at a local authority
- validate our assumptions

We want to understand where our effort is best spent.

What we did

Our research approach - a breakdown

We conducted



Desk research

Stakeholder interviews



10
organisations



13
participants


We analysed




163
local authority responses to a ransomware survey

Local authority interviews

Interviewee selection
We selected local authorities who scored higher and lower on the ransomware survey to reflect a range of IT practices.




3
participants scored **higher**




2
participants scored **lower**

in relation to NCSC's **'Four tips for mitigating malware'**


We spoke to




5
Local Authorities*




8
Participants



1
City Council



3
Borough Councils



1
Shared Services

Ransomware survey

Following recent ransomware attacks at local authorities, MHCLG (working with NCSC and the Cabinet Office) compiled a survey for local authorities.

The questions were generated around NCSC guidance from the '[Mitigating Malware and Ransomware Attacks](#)' publication, which includes four tips:

Tip 1
Make regular backups

Tip 2
Prevent malware from being delivered to devices

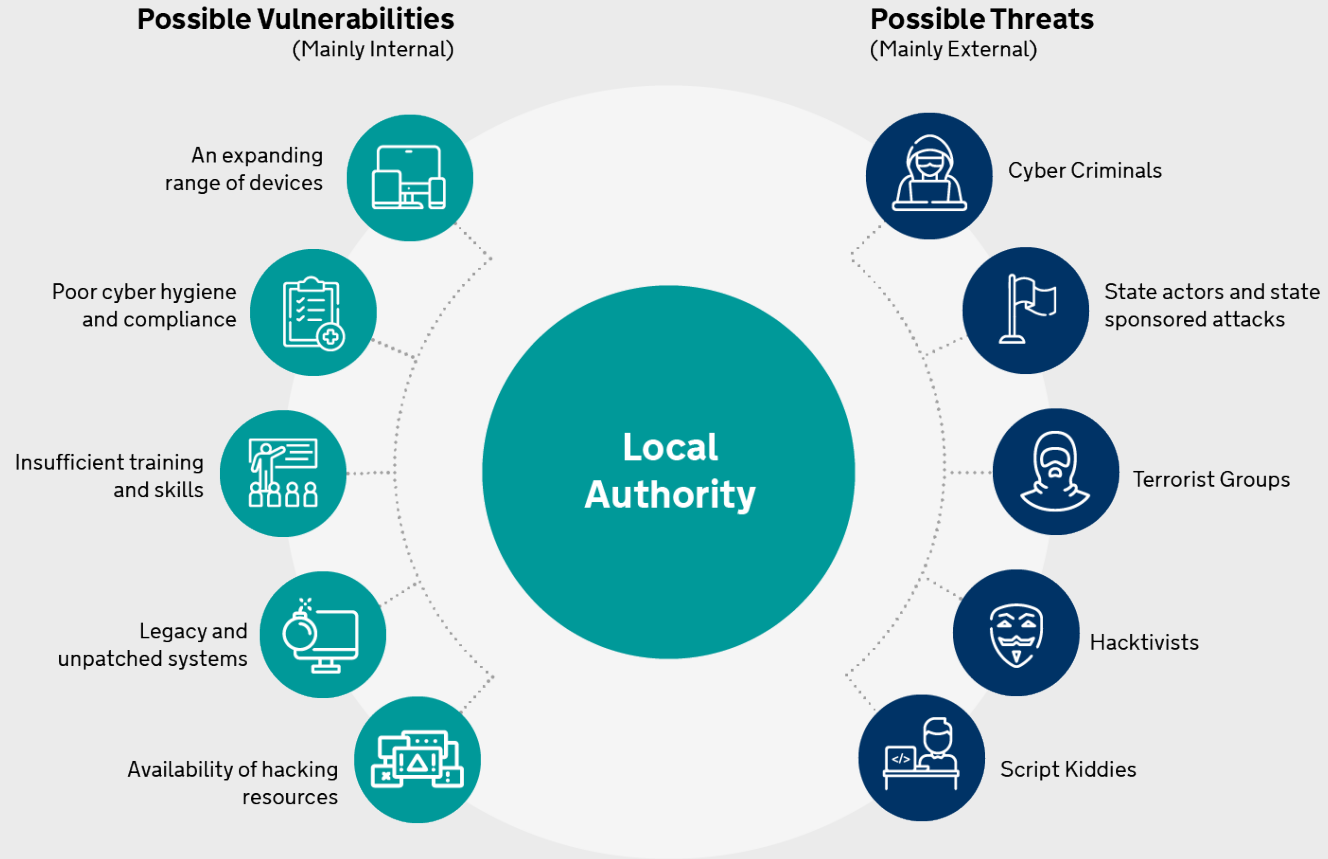
Tip 3
Prevent malicious code from running on devices

Tip 4
Limit the impact of infection and enable rapid response

What we learned

Possible threats and vulnerabilities at a local authority

The National Cyber Security Strategy (NCSS) categorises cyber risks into 'vulnerabilities' and 'threats'.



Cyber security is a complex area

It is simpler to consider three phases in incident management:



Protecting against a cyber attack

Taking a 'secure by design' approach protects against potential attacks, data breaches and any impact on the citizens that use services.

About this section

The following observations are reflections of user feedback and opinions.

We collectively analysed findings to create the report and to generate hypotheses.

Protecting against a cyber attack

These organisations provide services, guidance and support to local authorities in building and maintaining secure services.

[View more detail](#)

	Services	Advice & Guidance	Training	Funds	Support Network	Technology
MHCLG			●		●	
LGA	●			●	●	
NCSC	●	●	●			●
WARPS		●	●		●	
GDS	●					●
NHS Digital						●
LRFs	●					
EPC	●		●			
RED						
Gov Security Group						

The themes we uncovered

As the pre-discovery progressed we saw evidence emerge within certain themes.

We found a wide variety of evidence - both good and not so good practice - reflected within these themes.

We have grouped the following evidence using these themes.



There is no consistent understanding of what cyber security entails or means for a local authority, making consistent prevention more difficult

There is inconsistency as to what constitutes a breach.

Some stakeholders felt that information management is separate to cyber security, however the National Cyber Security Strategy includes information management.

There is a perception that cyber security and risk relates solely to penetration testing, defending against hackers and defending against virus threats.

We believe that this is an incomplete perspective, as cyber risk extends to the systems, the data kept in the systems, the hardware used to access the systems, and the services provided.



If there's a conversation to be had in MHCLG regarding Office 365 configs in local authorities, for example, standards that MHCLG want to consider looking at, advice around what good looks like in Office 365. We could provide a template of what Office 365 looks like when it's well configured and MHCLG could promote it to local authorities.

- **Organisation 03**

Local authorities have differing opinions of what good cyber security looks like

What good cyber health and maintaining good cyber health looks like is unclear.

Some stakeholders and users feel that being PSN-assured means that a council is cyber secure.

Cyber security means different things to different people.

“

I think the sector is disadvantaged as it doesn't have anyone setting that governance, e.g DFT set governance for transport and aviation so regulation is in place. BEIS regulates power so that gets done. No one regulates local authorities.
- **Organisation 03**

Awareness of cyber security risk often varies within a local authority

Cyber security awareness appears to vary by length of experience and job function.

Non-IT council staff and councillors are unaware of their responsibilities in contributing to cyber health.

Within the IT department, cyber security is seen as a specialist sub-area.

In one case, we heard that some councillors were unhappy with the cyber security measures put in place regarding device management and application access.

“

The SLT board, except the Director, are not very cyber security aware.

- **Local Authority 05**

Cyber security is seen as an IT risk, not a business risk

Users see cyber security as belonging to IT.

Cyber security does not get the attention or funding it needs at senior levels to ensure proper resource allocation.

The risk of cyber gets passed into ICT risk registers, rather than put into the business risk register. This leads to a higher risk of poor cyber security practices and can lead to a lack of ownership from senior leaders.

Board level non-IT staff have less cyber security awareness. This lack of awareness leads to cyber security being perceived as a lower priority at board level, and therefore less resources are allocated to mitigation activity.

“

The message needs to be hit home. If senior leadership teams were [more] aware of financial and reputation damage, maybe they would change.

- **Organisation 03**

Different levels of priority and funding are allocated to cyber security within councils

Local authorities intend to perform activities that will improve cyber health, whereas IT leaders can find themselves constrained by budget competition in their organisation.

Councils are at differing levels of cyber health due to resourcing and prioritisation issues.

One stakeholder said that:

- A third of local authorities have the resource and knowledge to improve.
- Another third have not got the resource to improve, but are trying their best.
- The last third do not know about cyber security and do not feel it is a priority.

“

Local authorities still have legacy IT systems largely because of finance constraints or they are on a cycle of updates.

- **Organisation 01**

Knowledge of incidents affecting other local authorities helps to focus attention on cyber security

Recent incidents have enabled those responsible for managing security risk on a technical level (IT managers) to escalate and push cyber security onto the agenda of senior leadership teams.

Users feel that information about previous incidents helps frame the cost, impact and fallout of cyber security risk for senior stakeholders.

“

Cyber security has been brought quite firmly into focus with [recent incidents].
- **Local Authority 03**

Information sharing networks are not just useful for upskilling, but also for procurement and network building

Different groups and organisations have been established to collaborate, share information and skills between peers and local authorities.

WARPs are useful for collaboration and network building. They may operate differently, which could impact their effectiveness.

There is a wide variety of skill levels and capability needed to join and contribute to discussions at WARPs.

IT professionals working in or around cyber security appreciate being given opportunities to gain support from peers in tackling cyber security issues.

“

Information sharing is good, as if something's going on, people need to know about it - because it could happen to them next.

- **Organisation 03**

Information sharing networks are seen as useful and flawed

Networks such as WARPs are seen as effective tools for sharing information.

WARPs have problems and could be strengthened.

Some councils have set up their own networks to facilitate information sharing and best practice.



WARPS need a lot of work around standardisation and making them more effective. Standards e.g. membership fees, charter, what are they for.

- Local Authority 05



Some regional WARPs are good at some teaching things, but they don't share with others that are not so technically advanced in that area.

- Organisation 05

Analysis of cyber security risk is inconsistently completed when procuring non-IT and IT services

Users feel that third party services are often not assessed for their cyber security.

Councils do not know what good cyber security looks like or what the standards mean when purchasing contracts.

Ineffective supplier and contract management can lead to delivery delay. This leads to a persistence of legacy technology, which can result in increased cyber risk.

“

There was no cybersecurity person on panel when prospective service suppliers interviewed (just NCSC guidance provided).

- Local Authority 01

“

I would say cyber security isn't considered in non-IT procurement. It's a bit of a loophole there.

- Local Authority 05

Joint procurement of IT and cyber security contracts by local authorities is inconsistent

Joint procurement of IT and cyber security contracts by local authorities is seen as useful for economies of scale, but is sporadic and hard to achieve.

Small councils feel they have to wait for county councils (with bigger budgets) to procure cyber security or IT contracts.



There is no joint procurement as the county has a massive budget hole, so they're not really interested in the districts and boroughs.

- Local Authority 04

There is a misperception around standards and guidance

PSN is misperceived as an accreditation, and there is a misconception that membership equates to being 'cyber secure'.

It is unclear to local authorities what is guidance and what is a mandatory standard they have to meet.

Local authorities would like more direction from MHCLG.

IT staff are unsure of best practice, such as in server provision, and would welcome more guidance/intervention/audits from trusted sources.

Mandatory technical standards feel easier to enforce than suggested guidance.

“

PSN is nearing the end, who's gonna fill their gap with standards after?
- **Local Authority 01**

There is a wide variety of services and groups available to support and help, which can cause confusion for some users

There are a lot of organisations offering services, products and guidance to local authorities to manage their cyber security. This can cause confusion for some users.

The separation of roles between the NCSC, LGA, ICO and MHCLG is unclear in terms of how they support local authorities with cyber security.

“

NCSC do a good job of updating us and then it is what comes through from county each month for the general things, then it's just what we see.

- **Local Authority 05**

“

I don't think the ICO ever gets involved.

- **Organisation 05**

There is varying understanding of what tools are available, where to find them, and what they are for

A lot of products are available to help support councils with cyber security, but they are inconsistent in their take-up and use.

We found this across both the ransomware survey and feedback from users.



You could buy tech but you're relying on an IT manager who may not be up to date, or may not have the time to research it...

- **Organisation 02**

Moving away from legacy IT systems can be difficult

Local authorities lack the resources to be able to move away from legacy systems for a variety of reasons, including:

- people
- skills
- funding
- resistance to change
- prioritisation of user training

“

Time and money limitations have prevented us moving away some from legacy operating systems.
- **Local Authority 04**

There is a good take-up of NCSC services that help local authorities understand the threat landscape and better protect themselves

There is a good take-up of NCSC services, such as WebCheck, MailCheck and Protected DNS, among local authorities.

The majority of responding local authorities use the CISP information sharing platform.

“

NCSC do a good job of updating us and then it is what comes through from county each month for the general things, then it's just what we see.

- **Local Authority 05**

Local authorities lack sufficient numbers of IT staff who are trained in cyber security

Current user research continues to support previous research studies, in that “training and awareness of cyber security issues and arrangements offer the greatest opportunity for improvement” (LGA cyber security stocktake, November 2018).

Some local authorities are taking advantage of the LGA budget to upskill relevant employees, for example through apprenticeship schemes.

“

All employees get a couple of hours training on cyber security (to prevent attacks). It’s one-off and not mandatory.

- **Local Authority 05**

Central government's training offer for local authorities is limited

Pathfinder is the only centrally funded (as far as we're aware) cyber training programme that is available to local authorities to freely attend.

Pathfinder is mostly pitched at IT people, focussing primarily on process and strategy.

The impact of Pathfinder on cyber health has not been assessed once delegates return to their organisation.

Many local authorities depend on the private sector to upskill their organisation.

“

Training exists. People don't know it's there, for example from NCSC.
- **Organisation 05**

“

There needs to be more awareness among general staff regarding the basic cyber risks.
Everyone should do mandatory cyber training, like health & safety.
- **Local Authority 05**

Training of general (non-IT staff) is considered inadequate

Training is conducted inconsistently between councils in terms of:

- course type
- whether training is mandatory
- how often training is undertaken
- depth of the course
- frequency of the course

Local authorities are unclear on what training should be provided to staff.

Local authorities are unclear on what is the best format for training staff.

Training that is not accessible or relevant to staff interests was thought to be less successful.

“

The all staff training is not sufficient. It should be every year, not a one-off - even just a couple of hours or online. It would raise awareness and make people think, such as about data protection.

- **Organisation 04**

“

People do get the training, but I'm not convinced all the training is particularly useful.

- **Organisation 03**

Responding to an incident

Timely and measured initial response to a cyber breach can reduce impact and aid investigation.

Responding to a cyber security threat

These organisations provide services, guidance and support to local authorities in responding to a cyber security incident.

[View more detail](#)

	Services	Advice & Guidance	Training	Funds	Support Network	Technology
MHCLG	●		●			
LGA			●	●	●	
NCSC	●	●	●			
WARPS						
GDS						
NHS Digital						
LRFs	●					
EPC						
RED	●					
Gov Security Group	●					

There are differing levels of understanding of who to communicate with, when and why, in response to an incident

There is inconsistency in how incidents are escalated internally.

There is inconsistency in how to trigger a multi-agency response.

The process of how to recover, and who (and why) to communicate with, is unclear.

“

If things go wrong, some people are better at sharing info than others.
- **Organisation 04**

There are a variety of different types and implementations of response plans, which are not always tested

Councils identify and report incidents in different ways, according to the Big Brother report (2018). Some councils record and report thousands of attacks to the NCSC, while others report none.

Councils are legally required to have a response plan for emergencies because of the Civil Contingencies Act ([see Appendix](#)).

Incident response plans are not always tested.

Timely information-sharing about incidents helps councils to act quickly to protect themselves

Local authorities want to be told about attacks quickly, so that they can act if necessary.

Local authorities want to be given enough information about how the attack happened so they can act quickly to modify their own systems if necessary.

“

[Incident] was in the news before we got to hear of it and it was very quiet as to what was happening. More information about attacks and current threats would be welcome.

- **Local Authority 04**

“

Information from a trusted source is the best way to pass on information about attacks. It needs to be something specific they can act on, not generic advice like ‘make sure you’re backed up.’

- **Organisation 01**

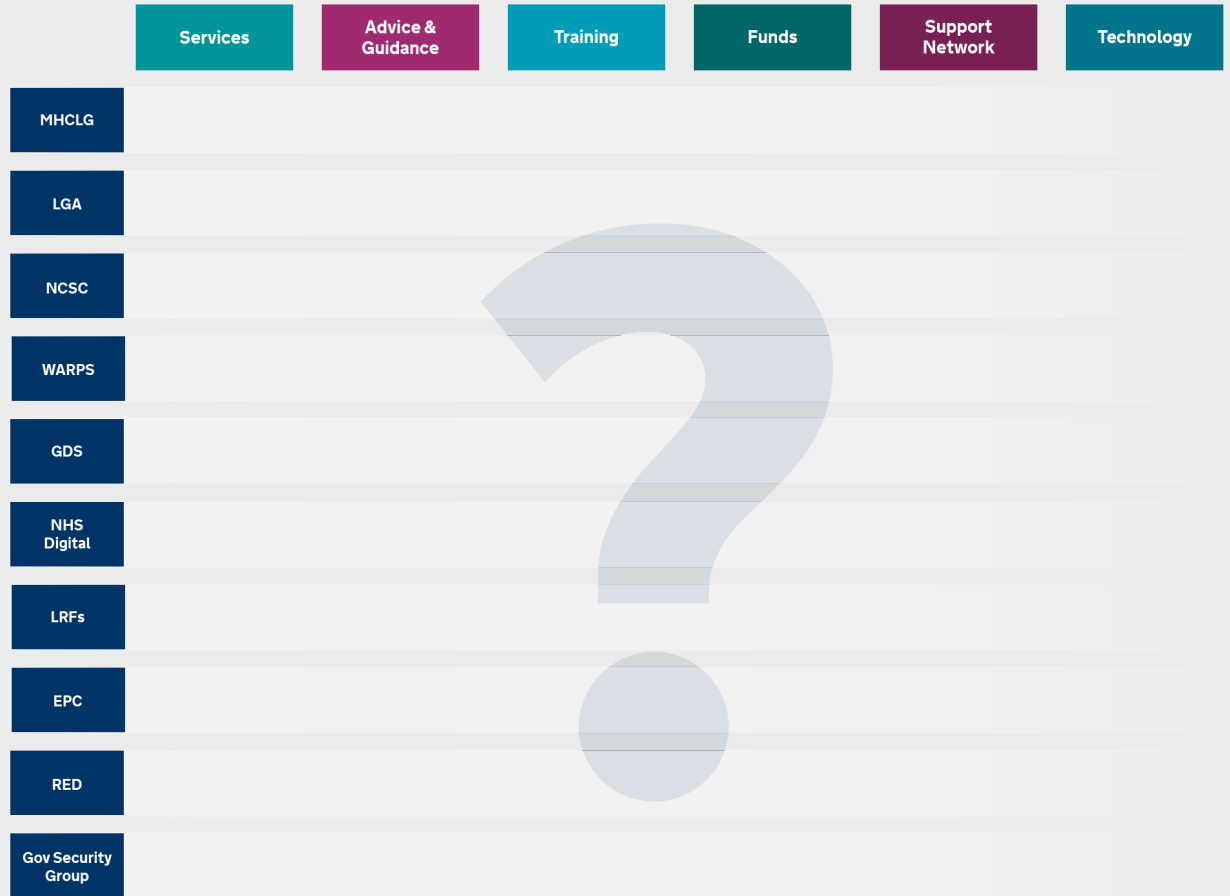
Recovering from an incident

Appropriate activities for successful recovery are enabled through pre-planning, technical preparation, practice and simulation.

Recovering from a cyber security incident

We found an imbalance in the support offered by organisations between the Prevent, Respond and Recover phases.

Support from external bodies appears to be reliant on the scale and impact of the incident and who was engaged during the incident response process.



Ransomware survey results

Technology areas of concern

The ransomware survey highlighted a number of councils that are not taking all available measures to reduce the risk of an attack.

Some of these relate to the regularity of IT health checks, use of legacy technology and the uptake of services offered by government.

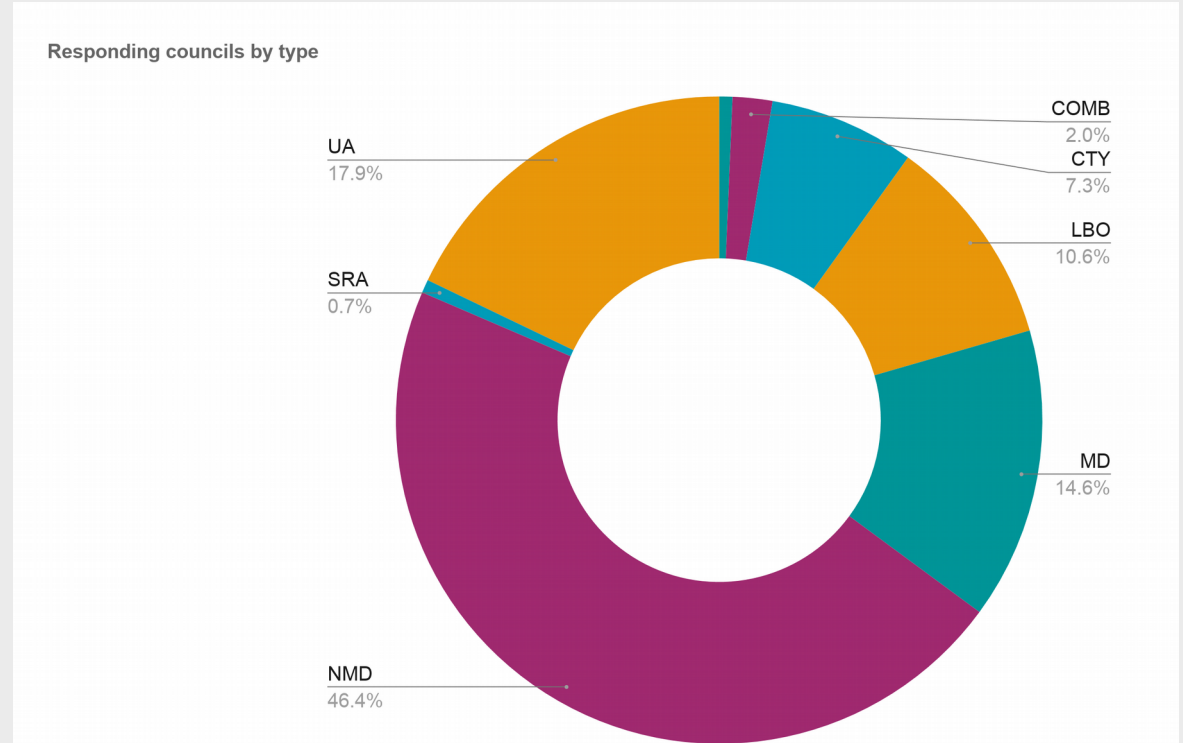
If you would like further detail of these results, please get in touch with the team on cyber@localdigital.gov.uk

Local authority responses

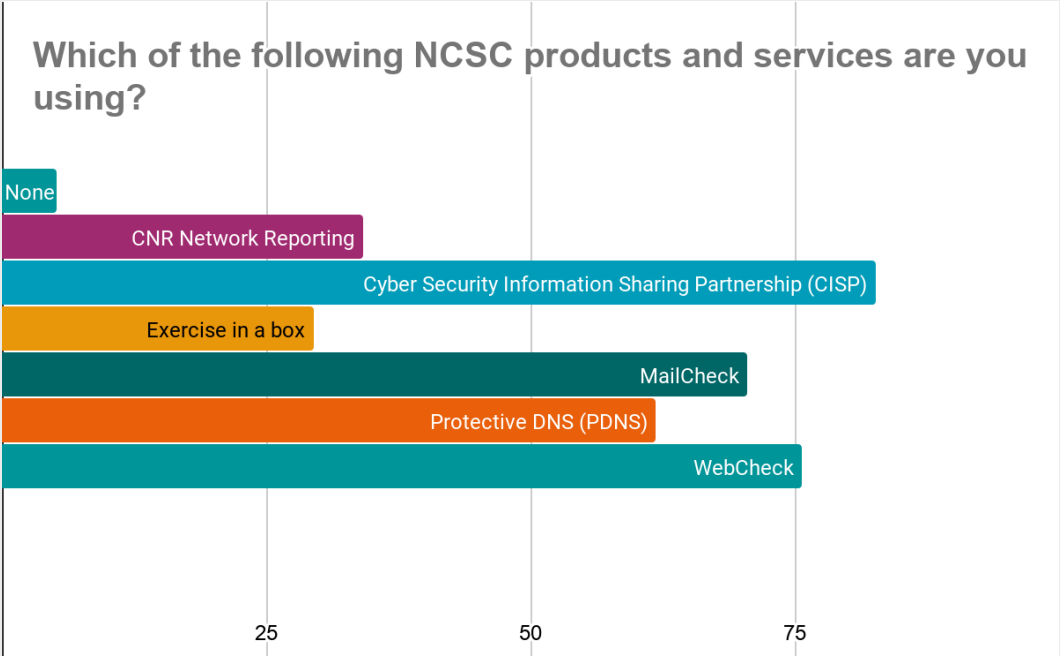
Just over half of all English local authorities responded to the Ransomware Survey.

The respondents were split across many different types:

- CTY: County Council
- COMB: Combined Authority
- LBO: London Borough
- MD: Metropolitan District
- NMD: Non-metropolitan District
- SRA: Statutory Regional Authority
- UA: Unitary Authority



NCSC Services



Hypotheses

We generated over 60 separate hypotheses, which we grouped into nine larger hypotheses/statements.

We then presented the hypotheses in a stakeholder workshop to help decide which to focus on during the next research phase.

Hypothesis 1.

Vulnerability to cyber attacks would be reduced if local authorities plan, build and maintain services in a secure manner

Cyber risk would be reduced if cyber security analysis is conducted across an entire user journey, service, data handoffs at the point of implementation, and delivery of products.

If the purchase of products is done using a 'secure by default' approach (for example, considering the full supply chain and lifecycle) then cyber risk would be reduced.

If cyber security is built into software, data handoffs and user touchpoints, you would not need to have cyber security training and could minimise the non-malicious risk posed by internal staff.

If cyber security is recognised as a business risk as well as an ICT risk, then organisations would start to consider cyber security in normal service delivery.

Hypothesis 2.

If all local authorities configured their technology appropriately, cyber security risk would be mitigated

If local authorities built cyber security and digital technology around staff and their needs, there would be less risk of a cyber security incident.

If all local authorities made use of NCSC services, there would be a reduced risk of attack.

The risks presented by outdated legacy infrastructure would be reduced through improved procurement practices.

If contract management was improved, legacy technology would be less prevalent. This would reduce cyber risk.

Hypothesis 3.

Allocation of resources (e.g budget and time) to cyber security would increase if it was a higher priority at board level

If ICT had a bigger voice at board level, it would be easier to raise awareness among senior management.

A bigger voice at board level would aid funding, budgets and priorities, and make it easier to justify ICT spend towards cyber security.

A community of professionals generates the power of many, not the few, which would help push cyber security onto senior management agendas.

If all local authorities had the same opinion of what good cyber security looks like, council peer pressure would lead to a higher level of cyber security across the board.

Hypothesis 4.

External organisation cyber security programmes for local authorities would be more effective if the information and risk picture of the sector was improved

If local authorities had the same triggers for a multi-agency response, this would create more effective England-wide spending due to the improved information and risk picture.

If we had a better idea of the amount of cyber incidents, it would be easier to quantify cost and type, allowing for a more proactive response to cyber security.

If local authorities were more consistent in identifying cyber incidents, it would give a more accurate sense of the scale and measures of current cyber risk.

If local authorities had the same triggers for a multi-agency response, a more representative picture could be built of the common occurrences that local authorities are experiencing.

Hypothesis 5.

Cyber security risk would be reduced if the behaviours, ownership and responsibility for cyber health at local authorities were improved

If awareness around cyber security risk was at the same level in each local authority, then behaviours and attitudes towards cyber security would change and everyone would begin to take ownership of it.

If cyber security was recognised as a business risk as well as an ICT risk, non-cyber staff and users would begin to take ownership of it.

If people took appropriate levels of ownership and responsibility for the role they could play in cyber security, then cyber security risk would be heavily mitigated.

Hypothesis 6.

Cyber security would increase within local authorities if they subscribed to clear standards, expectations and goals

If local authorities had the same triggers for a multi-agency response, a response would be more predictable and effective. It would also enable local authorities to see trends in attacks, and to improve and create services in response.

If good cyber technical practices were identified, mandated and maintained, local authorities would have to address cyber security risks.

If local authorities all had the same opinion on what good cyber security looks like, they would be able to adapt to current and changing guidance.

We should avoid the term 'standards' because cyber security is too dynamic and changing, while standards are fixed. Once a standard is reached, it becomes a KPI that has been hit and it falls off the roadmap.

If all local authorities had appropriate and tested incident response plans, it would better prepare them for a cyber security incident.

If cyber security was considered a standard practice for all procurement, the organisation would be safer.

Hypothesis 7.

Cyber security risk would be mitigated by improving the quality, networks and distribution of shared information

If the impact and costs of cyber incidents were shared, it would make cyber security a priority and raise awareness of the financial cost.

Regular, high quality information sharing about cyber security, vendors and risks would help local authorities to constantly maintain/limit the degradation of their cyber health, and lead to the ability to better respond to published threats.

If it was clearer who to communicate with for help and support, local authorities would be able to find more information about cyber security, have better incident responses and fewer incidents.

A community of professionals generates the power of many, not the few, which may help encourage better knowledge sharing and increase purchasing.

Regular, high quality information sharing about cyber security, vendors and risks would lead to better awareness among local authority staff.

Hypothesis 8.

Cyber security risks at local authorities can be mitigated by increasing the understanding of what cyber security is

If there was a consistent understanding of what cyber security means for a local authority, it would make communication easier and they could better assess how to improve cyber security and achieve a more effective spend.

If there was a consistent understanding of what cyber security means for a local authority, it would be easier to identify shortfalls, and training could be more targeted and therefore more effective.

Staff do not have enough knowledge to support an effective cyber security response.

If each local authority was entitled to free, regular and suitable training, there would be a reduction in the likelihood of falling vulnerable to an attack, and staff would be better equipped to respond if they did.

Hypothesis 9.

Cyber security at local authorities would be increased by a better understanding of associated risks and cost savings

If cyber security was considered for all procurement, less risk would be accepted and less money would be wasted.

If the impact and cost of cyber incidents were shared, risk would be simpler to quantify.

If there was a method of quantifying the cost of reducing risk, cyber security could compete with conflicting demands.

If there was a consistent understanding of what cyber security means for a local authority, they could make better use of budget and staff, because they could identify their strengths and weaknesses.

If there was a method of quantifying cost, reducing risk would be prioritised appropriately.

Recommendations for further work

Workshop outcomes

The workshop: what we did and what we needed

We gathered together stakeholders from across central government, local government and other organisations.

We needed their opinion, input and knowledge to:

- feedback on our findings
- prioritise and select which hypotheses to take forwards
- provide suggestions for users to reach out to

With their input, we were able to identify three hypotheses as priorities.

Priorities

We recommend taking the following three hypotheses forward as a focus of work:

Hypothesis 1. 'Secure by design'

Vulnerability to cyber attacks would be reduced if local authorities build, plan and maintain services in a secure manner.

Hypothesis 5. 'Standards and guidance'

Cyber security risk would decrease at local authorities if they subscribed to clear standards, expectations and goals.

Hypothesis 6. 'Ownership, responsibility, accountability'

Cyber security risk would be reduced if the behaviours, ownership and responsibility for cyber health at local authorities were improved.

What could a potential discovery look like?

Hypothesis 1. 'Secure by design'

We would investigate in greater detail the role of cyber security and information managers within local authorities. We would look to understand cyber risk across a whole user journey (such as reporting a missed bin collection) to identify where we could help local authorities ensure they are creating a secure end-to-end service.

Hypothesis 5. 'Standards and guidance'

We would investigate in detail the standards and guidance around cyber, IT and technology setups, how users in local authorities currently apply them on a daily basis, and their impact.

Hypothesis 6. 'Ownership, responsibility, accountability'

We would look to understand the current behaviours and ownership around cyber security within local authorities. We would look to understand how (and if) these behavioural changes could impact on an organisation's cyber health.

Why these things and why now?

Hypothesis 1 ('Secure by design') is an aspirational goal. It would need to be addressed as a longer term programme in terms of how MHCLG supports local authorities with their cyber security.

One thing we have heard throughout our research and engagement is that there is no one solution to fixing the problems with cyber security. This hypothesis has enough scope to allow us to explore and understand the problems and their solutions.

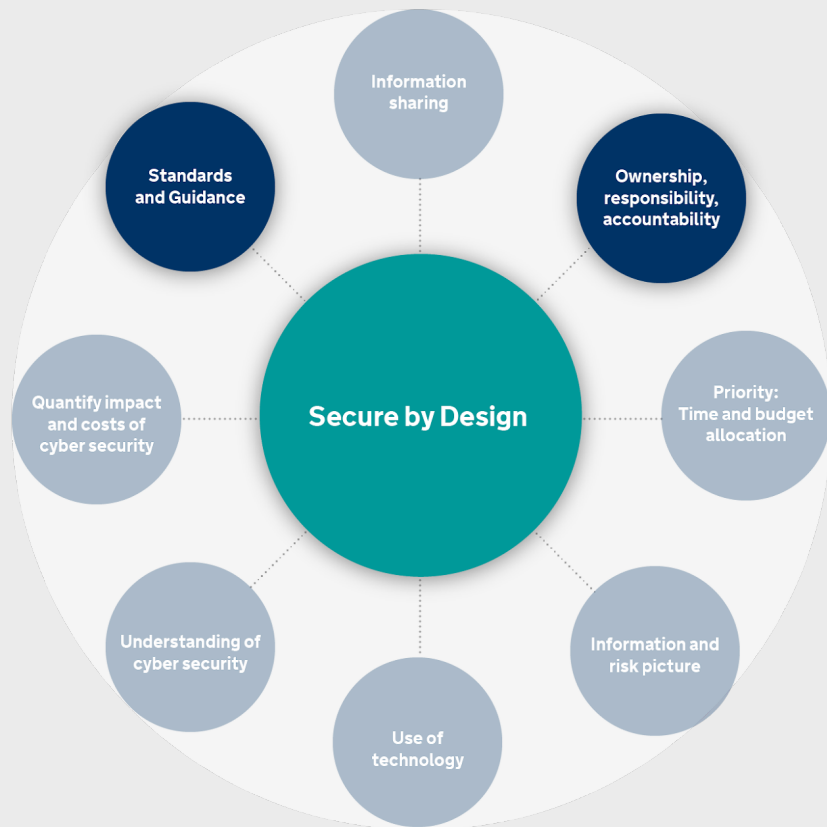
Hypothesis 5 ('Standards and guidance') and **Hypothesis 6 ('Ownership, responsibility, accountability')** are two concrete hypotheses that are easier to begin to research, however the content and the solutions for these are more unclear.

Research has indicated that these are fundamental questions that need to be examined in order to understand cyber security at a local authority.

What next?

‘Standards and guidance’ and ‘Ownership, responsibility, accountability’ are supporting components of ‘Secure by design’. They were selected through the stakeholder workshop to provide a direction for future research.

During this research and discovery we might find further relationships and dependencies between the remaining hypotheses and themes.



Gaps and limitations

What we would have done

There are several things we feel may have enhanced our research and would like to consider in future discoveries.

We would have liked to:

- gain a greater understanding of current cyber security standards, including technical, assurance and governance
- gain a greater understanding of the context behind the quantitative ransomware survey responses
- know 'when we are done' as new themes are discovered
- speak to more users and stakeholders from a variety of roles
- achieve greater relationships, empathy and understanding through working in-person with stakeholders, rather than remotely
- gain a greater understanding of private sector service provision, tools and training

Appendices

Appendix A.

Understanding the landscape

The tables in this section illustrate which organisations create and provide their own services to support local authorities in protecting against, and responding to, cyber incidents.

Protecting against a cyber attack (expanded)

	Services and Products	Advice & Guidance	Training	Funds	Support Network	Technology
LGA	<ul style="list-style-type: none"> - Self Assessment Tools - Cyber Workshops 	N/A	N/A	Funds training for staff and change management	Offer informal support but not a formalised network offering	N/A
MHCLG	N/A	N/A	Pathfinder training includes prevention modules	N/A	Informally broker connections between councils	N/A
NCSC	<ul style="list-style-type: none"> - Active Cyber Defence Tools - CNR platform - Vulnerability Disclosure platform - NCSC Marketplace - NCSC Supplier Certification - Incident reporting framework 	<ul style="list-style-type: none"> - Risk Management Guidance - Protecting Bulk Personal Data - Digital Service Security Design - Technical guidance - Attack Prevention guidance - Minimum Cyber Security Standard - Hundreds of pieces of guidance 	Exercise in a box	N/A	N/A	<ul style="list-style-type: none"> - Protective DNS Service - Host box capability (only piloted in BAIS) - Threat info adaptors - Web Check & Mail Check
LCIO Council (SOCITM)	N/A	N/A	N/A	N/A	Network for council CIOs <ul style="list-style-type: none"> - Help disseminate advice and guidance - Help promote and encourage cyber programmes 	N/A
WARPS	N/A	Collaborative space for council cyber security professionals	Help with skill-sharing	N/A	Provide access to a professional support network	N/A
GDS	Looking to design a domain management service	N/A	N/A	N/A	N/A	Public Services Network (includes yearly assessments & standards)
NHS Digital	N/A	N/A	N/A	N/A	N/A	Tech standards required for certain data access
LRFs	Work together with EPC, and with councils, to plan for all types of emergencies, including cyber	N/A	N/A	N/A	N/A	N/A
EPC	Work together with LRFs, and with councils, to plan for all types of emergencies, including cyber	N/A	Provide emergency training consultancy	N/A	N/A	N/A

Responding to a cyber security threat (expanded)

	Services	Advice & Guidance	Training	Funds	Support Network
MHCLG	Working to provide high risk councils with backups	N/A	- Pathfinder training modules - Finack exercise	N/A	N/A
NCSC	- CISP Platform - Refer to approved third party supplier (in case of crisis)	The main provider of guidance on response	Provides online resources on how to respond to attacks	N/A	N/A
LGA	N/A	N/A	Provides fund for training & certifying individuals	Provided funds to Redcar for NCSS supplier	Provides support and helps facilitate
LRFs	Can invite help from central government	N/A	N/A	N/A	N/A
RED	- Manage response - Processes and templates followed	N/A	N/A	N/A	N/A
Gov Security Group	Working to provide high risk councils with backups	N/A	N/A	N/A	N/A

The National Cyber Security Strategy (NCSS)

The scope of the National Cyber Security Strategy covers, but is not limited to:

- central government
- industry, including public (such as utilities and transport) and private services (such as the finance and retail industry)
- private citizens, who are more affected by, and exposed to, cyber risk than at any time before
- education
- defence

About the NCSS:

- £1.9 billion government investment in cyber security for 2016 to 2020
- Created NCSC (from GCHQ)
- Investing in cyber throughout government
- Creation of two academic centres of excellence
- Investing and encouraging market forces to contribute to cyber security

Response legislation and guidelines

Having business continuity arrangements in place is a statutory duty for local authorities under the Civil Contingencies Act 2004.

The Civil Contingencies Act requires Category 1 responders (local authorities) to maintain plans to ensure that they can continue to deliver their functions in the event of an emergency, as far as is reasonably practicable. This includes cyber. Business Continuity ISO 22301 is acknowledged as a generic framework that is applicable across the public, private and voluntary sectors in the UK.

The National Resilience Standard outlines how Local Resilience Forums (LRFs) can achieve good practice with signposting to further guidance and supporting knowledge. They are a set of individual standards to establish a consistent means for LRFs and their constituent local responder organisations to assure their capabilities and overall level of readiness.

The standards are intended to guide continuous improvement against mandatory requirements, good practice and leading practice. Responder organisations can use them as a benchmark

Appendix B.

Ransomware survey: Summarise responses

Appendix C.

Pathfinder training

About Pathfinder

The Pathfinder training programme is funded by central government.

It was developed by colleagues collaborating across several organisations: Resilience & Emergencies Directorate (MHCLG), Civil Contingencies Secretariat (Cabinet Office), National Cyber Security Centre, Emergency Planning College and Local Government Authority.

It has run 62 events in total with 3,600 attendees.

Six modules were delivered at eight regional locations across England, including some 'Multi-Agency Cyber Exercise' events.

Appendix D.

Glossary

Glossary of Terms, Abbreviations and Acronyms

NCSC - National Cyber Security Centre

NCSS - National Cyber Security Strategy

NCSP - National Cyber Security Programme

PSN - Public Services Network

WARPs - Warning, Advice and Reporting Points

LRFs - Local Resilience Forums

LGA - Local Government Authority

ICO - Information Commissioner's Office

ICT - Information, Communication & Technology

SLT - Senior Leadership Team

CISP - Cyber Security Information Sharing Platform

OS - Operating System

Appendix E.

Bibliography

Bibliography

Case studies

[LGA Stocktake Report, Jan 2019](#)

<https://www.local.gov.uk/lga-cyber-security-stocktake-national-level-report>

[NCSC Guidance: Mitigating malware and ransomware attacks, Feb 2020](#)

<https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>

[Big Brother Watch: Cyber attacks in local authorities, Feb 2018](#)

<https://bigbrotherwatch.org.uk/wp-content/uploads/2018/02/Cyber-attacks-in-local-authorities.pdf>

[Cyber Incident Approach Framework for Local Government - Cyber Incident Approach Framework for Local Government](#)

https://www.researchgate.net/publication/336400438_Cyber_Incident_Approach_Framework_for_Local_Government_-_Cyber_Incident_Approach_Framework_for_Local_Government

Bibliography (continued)

Cyber Incident Approach Framework for Local Government - Cyber Incident Approach Framework for Local Government
<https://www.researchgate.net/publication/336400438> Cyber Incident Approach Framework for Local Government - Cyber Incident Approach Framework for Local Government

A framework to understand Local Government network environments from a cyber security perspective. Developing an open source tool kit for Local Government

<https://www.researchgate.net/publication/336390789> A framework to understand Local Government network environments from a cyber security perspective Developing an open source tool kit for Local Government

Local Leadership in a Cyber Society 2: Strengthening our technical resilience

https://www.stgeorghouse.org/past_consultations/local-leadership-cyber-society-2-strengthening-technical-resilience/

Appendix F.

Accessibility

Accessibility aims

We want as many people as possible to be able to read this report, so we have considered:

- use of colours, contrast levels and fonts
- the ability to navigate most of the report using speech recognition software
- the ability to listen to most of the report using a screen reader

We've also used language that is as plain English as possible to understand.

Lastly, we used an accessibility add-on called [Grackle](#) to check our progress as we went, providing enhanced usability: [Grackle gslides add-on](#).

We appreciate that some aspects of the report may not be accessible. If you would like a simplified version of this report, please contact cyber@localdigital.gov.uk.