BIG BROTHER WATCH

Cyber attacks in local authorities

How the quest for big data is threatening cyber security

A Big Brother Watch Report

February 2018

Contents

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation. We hold to account those who fail to respect our privacy, and campaign to give individuals more control over their personal data. We produce unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

Contact

Jennifer Krueckeberg

Lead Researcher

Email: jennifer.krueckeberg@bigbrotherwatch.org.uk

24hr media line: 07505 448925

www.bigbrotherwatch.org.uk

Executive Summary

Local authorities are holding ever-expanding troves of personal information about citizens. Under the banner of data-driven government, they are seeking to actively gather more information about people. So-called 'smart cities' are armed with sensors and cameras that amass data about citizens, introducing a new level of everyday surveillance in the UK.

This accumulation of big data evokes not only concerns about ethics, rights and violations of privacy, but also about how equipped councils are to protect citizens' sensitive data. The number of serious cyber attacks is forecasted to significantly rise in the near future, making cyber security risks a clear priority. But is cyber security being appropriately prioritised by local authorities, or is more data collection the main focus of their digital strategies?

Based on Freedom of Information requests, Big Brother Watch found that UK local authorities have experienced in excess of **98 million cyber attacks over 5 years**. This means that there are at least **37 attempted breaches of UK local authorities** every minute. In addition, **at least 1 in 4 councils experienced a cyber security incident – that is, an actual security breach** - between 2013 – 2017.

While some councils have taken measures to face the ever growing threat from cyber attacks, especially the areas of staff training and reporting of successful cyber attacks need urgent attention.

In 2015, Big Brother Watch exposed how local authorities commit 4 data breaches a day, predominantly caused by human error.[1] Surprisingly, our current investigation reveals that little action has been taken to increase staff awareness and education in these matters. We found that **75% of local authorities do not provide mandatory training in cyber security awareness** for staff and **16% do not provide any training at all**. Considering that the majority of successful cyber attacks start with phishing emails aimed at unwitting staff,[2] negligence in staff training is very concerning and only indicative of the low priority afforded to cyber security issues.

Our findings further reveal that **25** local authorities experienced losses or breaches of data in the past five years as a result of **cyber security incidents**. Yet, **56% of councils** who failed to protect data from cyber security threats did not even report the incidents.

Big Brother Watch urges local authorities to review their policies with a view to mitigating the risks of cyber security incidents that threaten the security of citizens' invaluable data.

---

[1] Big Brother Watch (2015): A Breach of Trust – How local authorities commit 4 data braches every day https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/08/A-Breach-of-Trust.pdf

[2] Conner, Bill (2016): A Constant Threat: The Persistence Of the Email-Borne Cyberattack https://www.forbes.com/sites/forbestechcouncil/2017/08/18/a-constant-threat-the-persistence-of-the-email-borne-cyberattack/#4bbc82042b08

Policy Recommendations

1. **Local authorities must appropriately prioritise their cyber security.** Instead of investing in surveillance technologies, councils should invest resources on the development of cyber security strategies and the training of staff.

2. **Cyber security incidents should be consistently reported.** Local authorities need to establish a simple protocol that allows them to report incidents to the right authorities, whether the police, Information Commissioner's Office or the National Cyber Security Centre. This would ensure that threats are dealt with appropriately and that authorities' propensity to attacks is monitored. Furthermore, local authorities should utilise the National Cyber Security Centre's definitions of cyber attacks and cyber security incidents to ensure consistent reporting.

3. **All staff should receive mandatory training in cyber security.** Cyber attacks are not only designed to breach computer systems, but also to exploit humans who are often the weakest cyber security link. The ability to identify threats must not be reserved to ICT specialists but spread throughout the staff body. With large and ever-increasing volumes of data at stake, all local authority staff should have basic cyber security awareness.

Key Findings

Based on responses from 395 local authorities, equivalent to 94.5%

- UK local authorities have been subjected to at least **98 million** cyber attacks[3] between 2013 and 2017
- **114 (29%) councils** experienced at least one cyber security incident[4] - that is, an actual security breach - between 2013 and 2017
    - There were **376** cyber security incidents in total
    - **25 councils experienced** one or more cyber security incidents that resulted in the **loss or breach of data**
    - **More than half of councils (56%)** who experienced a loss or breach of data did not report it
- **297 authorities** (**75%**) do not provide mandatory training in cyber security
- **62 (16%)** councils do not provide any cyber security training

[3] A 'cyber attack' is defined by the UK's National Cyber Security Centre as 'a malicious attempt to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means

[4] A 'cyber security incident' is defined by the UK's National Cyber Security Centre as 'a breach of a system's security policy in order to affect its integrity or availability or the unauthorised access or attempted access to a system'

Tables

Table 1: Top 5 local authorities with highest number of cyber security incidents

No.	Council	Total cyber security incidents
1	Tonbridge and Malling	62
2	Herefordshire	22
3	Rhondda, Cynon, Taff	18
4	City of Edinburgh	11
5	Leicestershire	10

Table 2: Local authorities that experienced data breaches/losses due to cyber security incidents

Council	Total cyber security incidents that resulted in loss or breach of data
Merton	3
Westminster	3
Dacorum	2
Lincolnshire County Council	2
Derby	2
Canterbury	2
Warwick	2
Shetland	2
Tonbridge Malling	2
Rochford	1
Amber Valley	1
Mansfield	1
Hammersmith and Fulham	1
Lambeth	1
Blackpool	1
Hampshire	1
Gloucester	1
Taunton Deane	1
Medip	1
Wiltshire	1
Dundee City	1
City of Edinburgh	1
Conwy	1
Wrexham	1
Newry, Mourne and Down	1

The quest for data

Local authorities are important institutions that deliver a wide range of essential services. Councils provide 80% of all local public services,[5] playing a vital role in the everyday lives of British citizens. In light of their legal obligations and operational needs, councils collect extremely sensitive information about people - some of which relates to the most vulnerable people in society. The impact of the misuse or breach of such data can be severe for some. The data held by local authorities requires the highest of protection.

The need to meet a rising demand for services in the context of continued cuts, as well as the desire to innovate, is leading local authorities to embrace data-driven approaches. Local authorities hope new technologies will ease administrative burdens and improve engagement with the public while minimising expenses.

However, local authorities' applications of new technologies are now going far beyond simple modernisation initiatives. Many authorities have realised that the enormous and growing amount of public data they hold can be 'made use of'. Everything from social care for vulnerable children, waste collection, and council tax collection to planning applications produces large amounts of data.[6] Thus local authorities apply algorithms to identify areas in which they should invest more to better respond to citizens' needs.[7] This could mean, for example, exploiting vast amounts of the public's data simply to assess whether an area needs more frequent waste collection.[8]

While this might sound like a sensible approach to solving issues that affect citizens, the tale of data-driven local governance has a much darker side to it. Like any other area where new technologies are introduced to collect and analyse large amounts of personal data, serious concerns about people's privacy and security need to be addressed.

In order to gain valuable data, sensors, apps and cameras are deployed to track people's movements in real time – often without our knowledge or consent. Cities like Bristol, London, Manchester, Birmingham, Leeds and Milton Keynes are all in the race to become Britain's

[5] Blackwell, Theo (2017): Start of the Possible – digital leadership, transformation and governance in English local authorities, p.4 https://www.lgiu.org.uk/wp-content/uploads/2017/04/Start-of-the-possible.pdf
[6] Symons, Tom (2016a): Councils and the data revolution: 7 ways local authorities can get more value from their data. https://www.nesta.org.uk/blog/councils-and-data-revolution-7-ways-local-authorities-can-get-more-value-their-data
[7] Symons, Tom (2016b): Wise Council – Insights from the Cutting Edge of Data-Driven Local Government, p.20. https://www.nesta.org.uk/sites/default/files/wise_council.pdf
[8] Symons, Tom (2016a), op.cit.

smartest city,[9] which often comes with attractive funding from industry partners and investors.[10]

Milton Keynes, for example, has partnered with the Open University and businesses to create the MK Data hub. The project aims to collect and share data between stakeholders so they can use it for 'innovating' the city's infrastructure: "*[T]hese include data about energy and water consumption, transport data, data acquired through satellite technology, social and economic datasets, and crowdsourced data from social media or specialised apps*".[11]

One of Milton Keynes' flagship projects is a 'MotionMap' which, with the help of sensors and cameras, analyses car park occupancies, congestion and how crowded local buses are. Citizens are also encouraged to provide information about their location and movements with the promise that this data will be anonymised. However, numerous studies have shown that de-anonymising data is a serious risk that is difficult to mitigate,[12] and so zealous data sharing comes with real risks. Data collected by IoT ('Internet of Things') devices is especially difficult to anonymise[13] without rendering the data useless for analysis. Obtaining someone's birth date, gender and postcode can be enough to reveal their identity - and the more data available, the easier it is to identify a person.

The expansion of surveillance technology in public spaces is an attack on citizens' privacy and it creates security risks too. Collections of data troves about our every step and daily habits are attractive targets for criminals. Information held by councils today is far more detailed, varied and voluminous than a decade ago. This change significantly raises the stakes for local councils' cyber security. Should a council's cyber security be compromised in the near future, an enormous and detailed amount of sensitive data could easily fall into the wrong hands.

Our Freedom of Information request revealed that Milton Keynes council experienced 3 cyber security incidents between 2013 - 2017. Although none of the incidents caused a breach or loss of data, they demonstrate that local authorities have already drawn attention to the data they hold.

---

[9] Barber, Lynsey (2017): London's no longer the UK's top smart city as Bristol overtakes http://www.cityam.com/274393/londons-no-longer-uks-top-smart-city-bristol-overtakes

[10] Woods, Eric; Alexander, David; Rodriguez Labastida, Roberto; Watson, Rowan (2016): UK Smart Cities Index – Assessment of Strategy and Execution of the UK's Leading Smart Cities, p. 8 https://www.huawei.eu/sites/default/files/Huawei_UK_Smart_Cities_Report.pdf

[11] MK:Smart website: http://www.mksmart.org/about/

[12] Ebersold, Kyle and Glass, Richard (2016): The Internet of Things: A Cause for Ethical Concern, p.147 http://www.iacis.org/iis/2016/4_iis_2016_145-151.pdf

[13] Peppet, Scott R. (2014): Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, p 93 https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf

However, while the enthusiasm to integrate new data-driven technologies into public services is growing among council leaders, so are concerns over their ability to fend against cyber attacks. A survey by PwC Global CEO[14] found that only 53% of councils in the UK felt they were prepared to deal with cyber attacks and only 35% of council leaders felt confident that their staff had the necessary skills to deal with such threats.

With increasing data collection by local authorities, councils bear more responsibility to protect citizens' data. Their excessive use of surveillance technology under the smoke screen of innovation is not only an assault on citizens' privacy, but also a threat to their security.

Policy recommendation 1

Local authorities must appropriately prioritise their cyber security. Instead of investing in surveillance technologies, councils should invest resources on the development of cyber security strategies and the training of staff.

[14] Eichler, William (2017): Majority of councils ' unprepared' for cyber attacks, survey reveals https://www.localgov.co.uk/Majority-of-councils-unprepared-for-cyber-attacks-survey-reveals-/43327

What are cyber attacks and what damage can they do?

There are different motivations behind cyber attacks. Many are committed by criminals that want to gain information or financial rewards, but they can also be politically motivated, used for espionage, to disrupt infrastructure, or simply executed to embarrass local authorities.

According to the responses we received to our FOI requests, the most common types of cyber attacks were:

- malware: malicious software like computer viruses, worms, Trojan horses, ransomware, spyware, scareware and similar programs, and
- phishing: attempts to obtain sensitive information like usernames, passwords or credit card details.

Furthermore, ransomware attacks like the WannaCry attack of May 2017 are likely to become more frequent in the near future. Ciaran Martin the Head of the National Cyber Security Centre (NCSC) said recently in an interview "it is a matter of when, not if" a major cyber attack will happen in the UK.[15]

"At least 98 million cyber attacks on local authorities took place between 2013 - 2017"

This warning also applies to local authorities as they are becoming attractive targets, possessing growing volumes of information of interest to malicious cyber attackers.[16] The frequency of cyber attacks is a concern, but the potential impact of an attack means that even a single breach can be incredibly damaging and affect the lives of thousands of people.

Gloucester City Council was fined £100,000 by the Information Commissioner's Office (ICO) after a cyber attack exploiting the 'Heartbleed' software flaw in 2014 led to a significant breach of council employees' sensitive personal information. Despite repeated warnings about the Heartbleed vulnerability, the council had not addressed it. Subsequently, over 30,000 emails

[15] MacAskill, Ewen (2018): Major cyber-attack on UK matter of 'when, not if' – security chief. https://www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin

[16] Department for Communities and Local Government (2015): Understanding Local Cyber Resilience – A guide for local government on cyber threats and how to mitigate them, p.4 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/429190/Understanding_local_cyber_resilience.pdf

were downloaded from council mailboxes containing financial and sensitive information.[17] In the response to our FOI request, Gloucester said: "The single incident impacted one desktop and infected approximately 30,000 files, all of which were recovered from backup."

This example illustrates how negligence in taking adequate cyber security measures can quickly lead to a serious cyber security incident. But it also shows that some local authorities do not understand the severity of such incidents – recovering files from a backup is helpful, but is no means the answer to this serious breach.

A constant threat

Our research reveals the number of cyber attacks against local authorities to be prolific. Our Freedom of Information requests found that 129 local authorities had experienced at least 98 million cyber attacks – this means that there are at least 37 attempted breaches every minute.

Are cyber security incidents reported?

As part of devolution processes local authorities have considerable autonomy with regard to how they handle their IT systems. Although it is good practice to do so, the Data Protection Act 1998 places no obligation on local authorities to report cyber attacks or cyber security incidents. The forthcoming EU General Data Protection Regulation (GDPR) will introduce a duty on all organisations to report an information security incident that is likely to result in a risk to the rights and freedoms of individuals to the ICO within 72 hours of becoming aware of it.

"56% of councils who experienced a breach or loss of data did not report it"

Cyber security incidents should be consistently reported. It is particularly worrying that 56% of local authorities that experienced a breach or loss of data did not report these at all.

The government guideline "Understanding Local Cyber Resilience" recommends local authorities to: "*(r)eport online crimes to the relevant law enforcement agency to help the UK*

[17] Information Commissioner's Office (2017): Gloucester City Council fined by ICO for leaving personal information vulnerable to attack https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/06/gloucester-city-council-fined-by-ico-for-leaving-personal-information-vulnerable-to-attack/

build a clear view of the national threat and deliver an appropriate response."[18] We agree with the ICO's recommendations that local authorities should, at the very least, "*develop a process for assessing and grading risk so that all qualifying incidents are reported appropriately to the ICO*" and that "*decisions as to whether or not to notify any incidents to the ICO should be noted on incident logs*".[19] This is vital for ensuring good practice and accountability.

Reporting cyber security incidents is crucial in building future resilience. Of the reports that were made, 33 cyber security incidents were reported to the Police; 17 to the ICO; 26 to the National Cyber Security Centre (NCSC); and 8 to the predecessor schemes GovCertUK and CERT UK.

Joining schemes like CiSP[20] as provided by the NCSC can help to share information about current threats across sectors, reduce the risk of harm and offer support to local authorities in case of an incident.

Policy recommendation 2:

Cyber security incidents should be consistently reported. Local authorities need to establish a simple protocol that allows them to report incidents to the right authorities, whether the police, Information Commissioner's Office or the National Cyber Security Centre. This would ensure that threats are dealt with appropriately and that authorities' propensity to attacks is monitored. Furthermore, local authorities should utilise the National Cyber Security Centre's definitions of cyber attacks and cyber security incidents to ensure consistent reporting.

[18] Department for Communities and Local Government (2015): Understanding Local Cyber Resilience – A guide for local government on cyber threats and how to mitigate them, p.11. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/429190/Understanding_local_cyber_resilience.pdf

[19] Information Commissioner's Office (2018): Findings from ICO information risk reviews of incident management at 10 local authorities, p.4 https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2173110/outcomes-report-local-authorities-incident-management.pdf

[20] National Cyber Security Centre website: https://www.ncsc.gov.uk/cisp

Training

A larger portion of incoming cyber attacks are blocked by IT systems and employing cyber security specialists is essential to keep systems safe. However, because attacks are often concealed in emails or links, any staff member connected to IT networks is a potential liability.

"75% of councils do not provide mandatory training in cyber security"

In 2016, Lincolnshire County Council was hit by a £1m ransomware demand. The malware spread through the IT systems because a user opened and shared an email they could not open. Although no data was stolen, systems were down for 3.5 days.[21]

Training staff in cyber security must be afforded due priority - particularly as criminals constantly adapt and innovate their strategies.

Government guidance states that local authorities: "*(p)roduce user security policies that describe acceptable and secure use of your organisation's ICT systems. These should be formally acknowledged in employment terms and conditions.* ***All users should receive regular training on the cyber risks they face as employees and individuals.*** *Security related roles (such as system administrators, incident management team members and forensic investigators) will require specialist training."*[22]

In addition, the ICO recommends that local authorities "*develop content and delivery of information incident security management training as part of* ***mandatory data protection induction training"*** which should be refreshed annually. We agree with the ICO that such training is "*critical to future GDPR proofing*."[23]

However, only 25% of local authorities reported having mandatory training on cyber security awareness. While some authorities reported offering annual or even bi-annual refreshers, many provide training only for new staff during induction. 16% of local authorities reported not having any training or to only use bulletins and messages via internal communications to disseminate advice. While internal communication is a valuable tool to update staff on an ad hoc basis, it is

[21] Lincolnshire County Council (2016): Malicious Malware (Cyber) Attack Presentation, http://istanduk.org/wp-content/uploads/2016/05/09g-lincolnshire-malware-attack-nottingham.pdf
[22]Department for Communities and Local Government (2015): Understanding Local Cyber Resilience – A guide for local government on cyber threats and how to mitigate them., p.11 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/429190/Understanding_local_cyber_resilience.pdf
[23] Information Commissioner's Office (2018): Findings from ICO information risk reviews of incident management at 10 local authorities, p.4 https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2173110/outcomes-report-local-authorities-incident-management.pdf

no substitute for the vital cyber security training required to protect authorities' networks and the vast amounts of data they hold.

Furthermore, more than half of councils either didn't have a specific budget on cyber security training or said they spent 0% on it. This lack of investment in training is mirrored by a separate FOI request submitted by cyber security company Citrix in 2016. Citrix found that local authorities only spent £3,378 on average on cyber security training compared to £27,818 on health and safety training.[24]

Every council has a duty to minimise the risk of a cyber security incident, which includes informing staff about the dangers and training them to act appropriately should one occur. We find it unjustifiable that local authorities have, by and large, failed to provide basic, vital cyber security training.

Data loss and major cyber security incidents have often been caused by human error - 90% of all cyber attacks begin with phishing emails.[25] Authorities should not only focus on putting robust technological protections into place, but also ensure that staff have the basic knowledge and training required to defend against the most elementary, potentially extremely harmful, attacks.

Prevention is better than cure and training staff properly in how to respond to cyber attacks, what to avoid and what to do if a cyber security incident occurs, should be the minimum to protect citizens' valuable data.

Policy recommendation 3:

All staff should receive mandatory training in cyber security. Cyber attacks are not only designed to breach computer systems, but also to exploit humans who are often the weakest cyber security link. The ability to identify threats must not be reserved to ICT specialists but spread throughout the staff body. With large and ever-increasing volumes of data at stake, all local authority staff should have basic cyber security awareness.

[24] Metzger, Max (2016): Councils spend nearly 8x more on health and safety training than IT security https://www.scmagazineuk.com/councils-spend-nearly-8x-more-on-health-and-safety-training-than-it-security/printarticle/568621/

[25] Conner, Bill (2016): A Constant Threat: The Persistence Of the Email-Borne Cyberattack https://www.forbes.com/sites/forbestechcouncil/2017/08/18/a-constant-threat-the-persistence-of-the-email-borne-cyberattack/#4bbc82042b08

Limitations

Curiously, 126 councils said that they did not experience any cyber attacks during the specified period. This seems highly unlikely.

These 126 councils did not report superior training – in fact, 28 of them (22%) reported not providing any cyber security training for staff at all. The Government guide "Understanding Local Cyber Resilience",[26] published by the Department for Communities and Local Government, states that "*33,000 malicious emails are blocked from accessing public sector systems every month.*" Given the general trends we discovered, the likelihood that some authorities were completely spared from any attacks is not plausible. Furthermore, 15 (12%) of the councils that reported no cyber attacks also said they experienced a cyber security incident.

It is possible that those 126 councils did not have regard to the definition of 'cyber attack' when responding to our request for information, further demonstrating a poor understanding of terminologies.

Additionally, we received several vague estimates about the number of cyber attacks local authorities had experienced in the past five years. Some local authorities stated that they experience hundreds or sometimes thousands of cyber attacks a day or a month. To include their data, we multiplied their lowest daily/monthly estimate to fit the five year window – for example, if an authority reported 'thousands of cyber attacks per day', we multiplied (1000 x 365) x 5 for a conservative five-year estimate. As a result of these vague responses, the figure we have reported of 98 million cyber attacks over five years is a conservative estimate.

[26] Department for Communities and Local Government (2015): Understanding Local Cyber Resilience – A guide for local government on cyber threats and how to mitigate them, p.4

Conclusion

Instead of implementing an increasing amount of surveillance technology and accumulating big data, councils should shift their attention to securing their systems and protecting citizens' data.

Our research suggests that local authorities are not taking cyber security and data protection seriously enough. While some councils have a developed good understanding of the danger cyber attacks pose, good practice needs to be seen across the board. It is unacceptable that living in the jurisdiction of a council with lax policies and insufficiently trained staff exposes those citizens' personal data to greater risk.

This report has demonstrated that failures to report breaches and training short-comings are part of this negligence. To quote a policy briefing provided by the Society of Information Technology Management (Socitm), *"Cyber resilience is generally seen as an 'IT security' matter in local government, not often treated as a major business and service threat, with top executive and political ownership. This needs to change."*[27]

Councils need to play their part in the UK's data ecosystem and do their best to prevent successful cyber attacks. With the risk only increasing over time, it is crucial that they act now before serious harm is done.

[27] Socitm (2016): Briefing – Role of local government in National Cybersecurity Strategy: A policy perspective from Socitm https://khub.net/documents/13043179/15867334/Socitm+Policy+briefing+-+Role+of+local+government+in+National+Cybersecurity+Strategy/3102bca6-24b2-4f36-a664-3fd5a4dfe76d

Appendix 1: Original FOI Request

Dear Sir or Madam,

I am writing under the Freedom of Information Act 2000 to request information about cyber-attacks and cyber security incidents affecting your authority. Specifically, I am asking the following for each year since 2013:

Please note: We are using the following definitions in accordance to guidelines given by the National Cyber Security Centre (NCSC). https://www.ncsc.gov.uk/incident-management

Cyber-attack: a malicious attempt to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means

Cyber security incident: a breach of a system's security policy in order to affect its integrity or availability or the unauthorised access or attempted access to a system

1. Please provide details of how many cyber-attacks to computer systems, networks or devices have taken place
2. Please provide details of how many cyber security incidents caused internal systems or devices to be infected or for services to be affected.
3. How many times have you reported cyber security incidents to:
   a) Police
   b) NCSC
   c) Information Commissioner's Office (ICO)
   d) Other, please provide detail
4. How many cyber security incidents have caused the loss/breach of data?
5. Please provide details of the cyber security awareness training provided to staff.
6. Please detail the number of staff trained in cyber security awareness.
7. Please detail what percentage of the annual budget has been allocated towards:
   a) securing IT-systems and networks against cyber-attacks
   b) training staff in cyber security awareness

I understand under the Freedom of Information Act that I am entitled to a response within twenty working days. I would be grateful if you could confirm this request in writing as soon as possible.

Appendix 2: Full Local Authority Breakdown

Council	Number of cyber attacks	Number of cyber security incidents	Number of reported cyber security incidents				Number of data breaches /losses	Training details	Number of staff trained in cyber security awareness	% of budget spent on cyber security	% of budget spent on cyber security awareness training
			Police	NCSC	ICO	Other					
Essex	731,910	0	0	0	0	n/a	0	Mandatory e-learning - additional guidance via regular communications	All staff	2014/2015 £ 559,429, 2015/2016 £660,413	Not possible to identify budget
Harlow	1	1	0	0	0	n/a	0	In the process of rolling out training - Weekly bulletins only	All staff	Financial Year 2013/14 1.75% Financial Year 2014/15 2.1% Financial Year 2015/16 2% Financial Year 2016/17 1.6% Financial Year 2017/18 1.45%	0%
Epping Forest	0	1	0	0	0	n/a	0	Mandatory training at induction	2 specialists	No specific budget allocated	No specific budget allocated

Brentwood	Refused: Section 17 and Section 31(2) Prejudicial to Law Enforcement										
Basildon	0	2	0	0	0	n/a	0	Mandatory training at induction - additional emails	All staff	No specific budget allocated	No specific budget allocated
Castle Point	Failed to reply to FOI										
Rochford	1	1	0	0	0	n/a	1	No training	n/a	£270,500 (total ICT budget)	n/a
Maldon	0	0	0	0	0	n/a	0	Mandatory training at induction - additional guidance via emails, intranet. Awareness tested periodically	All staff	Information not held	Information not held
Chelmsford	4	1	0	0	0	n/a	0	Information Awareness Week which includes cyber security	4 specialists	No specific budget allocated	No specific budget allocated
Uttlesford	Failed to reply to FOI										
Braintree	5	5	3	1	5	n/a	0	No details given	All ICT users	No specific budget allocated	No specific budget allocated
Colchester	1	1	0	0	0	n/a	0	No training - guidance via emails, splash screen and poster campaigns	All ICT users	Information not held	Information not held
Tendring	2	2	0	0	0	n/a	0	No mandatory training - guidance via email and phishing exercises	All staff	>1%	>1%
Thurrock	0	0	0	0	0	n/a	0	Mandatory e-learning	All staff	No specific budget allocated	No specific

											budget allocated
Southend-on Sea	4	4	0	0	0	n/a	0	Training at induction- additional guidance via workshops, emails, phishing campaign and posters	None	Not stated	Not stated
Cambridgeshire County Council	Refused: S12 Time and Costs										
Cambridge	1	0	0	0	0	n/a	0	No specific training - part of IT induction and Data Protection training	n/a	£192,347 (10.5% of software budget)	n/a
South Cambridgeshire	0	0	0	0	0	n/a	0	No specific training - part of IT induction and Data Protection training	n/a	£192,347 (10.5% of software budget)	n/a
Huntingdonshire	0	0	0	0	0	n/a	0	In the process of rolling out training	Information not held	£192,347 (10.5% of software budget)	Still being developed
Fenland	0	0	0	0	0	n/a	0	E-learning	All ICT users	7.40%	0.30 %
East Cambridgeshire	0	0	0	0	0	n/a	0	No training	None	approx. 5% of ICT budget	0%
Peterborough	IT services outsourced to Serco										
Norfolk County Council	6	6	0	0	0	Action Fraud, HP and PSN	0	Mandatory e-learning – part of Data Protection Essentials and Information Security	All staff	No specific budget allocated	No specific budget allocated
Norwich	564	1	0	0	0	n/a	0	Cyber Security Week - additional guidance via messages and security policy	All ICT users	Services outsourced	Information not held
South Norfolk	Refused: Section 31(2) Prejudicial to Law Enforcement										
Great Yarmouth	1	0	0	0	0	n/a	0	Annual training	All staff, 2 specialists	No specific budget	No specif

										allocated	ic budget allocated
Broadland	0	0	0	0	0	n/a	0	Training session held in early 2017	All staff	No specific budget allocated	No specific budget allocated
North Norfolk	0	0	0	0	0	n/a	0	No training - guidance via intranet and weekly briefings	5 specialists	approx. £37k	No formal training
King's Lynn and West Norfolk	0	0	0	0	0	n/a	0	Mandatory training at induction	2	3%	No extra costs - delivered in-house
Breckland	0	0	0	0	0	n/a	0	No details given	0	approx. 15%	0%
Northamptonshire County Council	Failed to reply to FOI										
South Northamptonshire	See response Cherwell										
Northampton	5	5	0	0	0	Local Government shared services	0	Not stated	Not stated	Not stated	Not stated
Daventry	0	0	0	0	0	n/a	0	Mandatory e-learning - additional guidance via intranet	All staff	No specific budget allocated	No direct costs
Wellingborough	0	0	0	0	0	n/a	0	No training - ICT user agreement only	All staff	Information not held	Information

											n not held
Kettering	No records held	0	Not stated	Not stated	Not stated	Not stated	Not stated	Training at induction - additional guidance via updates	Not stated, number of staff not recorded	No specific budget allocated	No specific budget allocated
Corby	0	0	0	0	0	n/a	0	No training	Not stated	No specific budget allocated	No specific budget allocated
East Northamptonshire	0	0	0	0	0	n/a	0	No training - ICT user agreement only	Refused	No specific budget allocated	Information not held
Suffolk County Council	1	0	1	0	0	n/a	0	No training - guidance via intranet	n/a	No specific budget allocated	No specific budget
Ipswich	Refused: Section 31(2) Prejudicial to Law Enforcement										
Suffolk Coastal	0	0	0	0	0	n/a	0	Training at induction - additional guidance via intranet	All staff	5.3%	0.5%
Waveney	See response Suffolk Coastal										
Mid Suffolk	Failed to reply to FOI										
Babergh	Failed to reply to FOI										
St. Edmundsbury	Failed to reply to FOI										
Forest Heath	Failed to reply to FOI										
Bedford	4	10> in each case	0	0	0	n/a	0	No training - Computer Security Policy and additional guidance via reminders	All staff	2013-14 0.023%; 2014-15 0.078%, 2015-2016 0.057%;2016-2017 0.449	2013-14 0.000%; 2014-15

											0.000 %, 2015-2016 0.000 %;2016-2017 0.003 %
Central Bedfordshire	0	0	0	0	0	n/a	0	Refused: Section 31(2) Prejudicial to Law Enforcement			
Luton	1	1	0	0	0	n/a	0	No training - guidance via internal awareness articles	Information not held	Information not held	Information not held
Hertfordshire County Council	over 6000 a day	Refused: Section 31(2) Prejudicial to Law Enforcement						Mandatory training at induction - additional guidance via intranet and workshops	All staff	8.5%	No specific budget allocated
Three Rivers	0	2	0	0	0	n/a	0	No training - guidance via email and intranet	All staff	£174k[28]	No specific budget allocated
Hertsmere	Refused: Section 31(2) Prejudicial to Law Enforcement										
Watford	0	0	0	0	0	n/a	0	Mandatory e-learning at induction	All staff	No specific budget allocated	No extra cost
Welwyn Hatfield	0	0	0	0	0	n/a	0	Mandatory training at induction	All staff	Information not held	Information not held
Broxbourne	0	0	0	0	0	n/a	0	No training - occasional guidance notes	n/a	No specific budget allocated	No specific

[28] Amount is for the financial year 2017-2018

											budget allocated
East Hertfordshire	Failed to reply to FOI										
Stevenage	2	2	0	0	0	n/a	0	Simulated email cyber security attacks, posters and guidance via emails	1200	approx. 10%	approx. 10%
North Hertfordshire	0	0	0	0	0	n/a	0	Not stated	Not stated	Not stated	Not stated
St. Albans	0	0	0	0	0	n/a	0	Cyber security sessions - additional training via phishing exercise and guidance via updates	All staff	Approx. 40% of ICT budget	0%
Dacorum	2	2	0	0	0	n/a	2	Training part of quarterly Data Protection course	285	Information not held in requested format	Information not held in requested format
Buckinghamshire County Council	4	0	0	0	0	n/a	0	In the process of rolling out training - Corporate policies to be signed only	Not stated	Service outsourced	Service outsourced
South Bucks	0	0	0	0	0	n/a	0	Mandatory e-learning	All staff	Information not available	Information not available
Chiltern	0	0	0	0	0	n/a	0	Mandatory e-learning	All staff	Information not available	Information not available
Wycombe	Failed to reply to FOI										

Aylesbury Vale	0	0	0	0	0	n/a	0	Mandatory e-learning - additional guidance via intranet	All staff (300)	Information not held in requested format	Information not held
Milton Keynes	3	3	0	4	0	n/a	0	E-learning - additional guidance via email briefings	2500	Information not held in requested format	Information not held in requested format
Lincolnshire County Council	605	2	2	1	0	n/a	2	Mandatory annual e-learning - additional guidance via internal communications, team presentations and meetings	4280 2016-2017; 1077 2017	Services outsourced	Services outsourced
Boston	1	1	0	0	0	Other local authorities connected to East Midlands Public Sector Network	0	No training - guidance via email and briefings	All staff	No specific budget allocated	No specific budget allocated
South Holland	0	2	0	0	0	n/a	0	No training - guidance via ad hoc messages	0	13/14 7.59%, 14/15 6.79%, 15/16 13.40, 16/17 12.54%	Not stated
Lincoln	2	2	2	2	2	n/a	0	No training - guidance via briefings, email and intranet	Not stated	Not stated	Not quantified
North Kesteven	0	0	0	0	0	n/a	0	No training - guidance via briefings and daily reminders	All staff	0.06%	0.08 %

South Kesteven	3	3	0	0	0	n/a	0	No training - periodical ad hoc messages	All staff	approx. 30%	15%
East Lindsey	0	2	0	0	0	n/a	0	No training - IT security policy and ad hoc messages	0	13/14 4.16%, 14/15 4.96%, 15/16 11.63%, 16/17 8.91%	Not stated
West Lindsey	Refused										
Derbyshire County Council	Information not held	0	0	0	0	n/a	0	No training - guidance via internet policy, procedures and publicity	Not stated	No specific budget allocated	No specific budget allocated
Derbyshire Dales	Refused: Section 31(2) Prejudicial to Law Enforcement										
South Derbyshire	2	0	0	0	0	Local Government Association	0	Mandatory training	All staff	Estimated 10%	0%
Erewash	0	0	0	0	0	n/a	0	Mandatory training	All staff	Estimated 10%	0%
Amber Valley	0	1	0	0	0	1 ENGWARP	1	Annual face-to-face training	250	0.05%	0.01 %
North East Derbyshire	Refused: Section 31(2) Prejudicial to Law Enforcement							Mandatory e-learning every 2 years	362	2.44%	No extra costs - delivered in-house

Chesterfield	4	3				1 GovCertUK	0	Mandatory e-learning at induction - all staff to complete annually	275	2013/14 (£9,063.18 / £14,728,760.00) = 0.06% 2014/15 (£22,394.05 / £13,888,650.00) = 0.16% 2015/16 (£108,839.83 / £14,203,610.00) = 0.77% 2016/17 (£97,305.79 / £14,001,700.00) = 0.70%	0%
Bolsover	Refused: Section 31(2) Prejudicial to Law Enforcement							Mandatory e-learning every 2 years	362	2.44%	No extra costs - delivered in-house
Derby	0	3	0	0	0	n/a	2	Mandatory e-learning at induction	All staff	Information not held	Information not held
East Staffordshire	0	0	0	0	0	n/a	0	E-learning - additional guidance via corporate policies, staff briefings and emails	All staff	No specific budget allocated	No specific budget allocated

Leicestershire County Council	13	10	0	0	0	n/a	0	Training part of Data Protection and Information Security training	All staff	No specific budget allocated	No specific budget allocated
Rutland	Refused: Section 31(2) Prejudicial to Law Enforcement										
Charnwood	9,269	0	0	0	0	n/a	0	E-learning at induction - part of Data Protection training	All staff	approx. 20%	<1%
Melton	0	0	0	0	0	n/a	0	No training - guidance via emails, briefings and notes	All staff	No specific budget allocated	No specific budget allocated
Harborough	Not recorded	3	0	0	0	n/a	0	E-learning - additional guidance via regular email briefings	All staff	Information not held in requested format	Information not held in requested format
Oadby and Wigston	0	0	0	0	0	n/a	0	No training - guidance via emails, briefings and notes	All staff	No specific budget allocated	No specific budget allocated
Blaby	0	0	0	0	0	n/a	0	No training - guidance via emails, briefings and notes	All staff	No specific budget allocated	No specific budget allocated
Hinckley and Bosworth	Refused: Section 31(2) Prejudicial to Law Enforcement										

North West Leicestershire	0	0	0	0	0	n/a	0	No training	None	£15,000	£5,000
Leicester	Refused: Section 31(2) Prejudicial to Law Enforcement										
Nottinghamshire County Council	0	0	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated
Rushcliffe	Refused: Section 31(2) Prejudicial to Law Enforcement							Annual e-learning - additional guidance via bulletins, spoof phishing campaign			
Broxtowe	Refused: Section 31(2) Prejudicial to Law Enforcement							E-learning - additional guidance via screensavers and email newsletter	All staff	30k per annum	No extra costs - delivered in-house
Ashfield	0	0	0	0	0	n/a	0	No specific training - online email awareness only	Not stated	No specific budget allocated	No specific budget allocated
Gedling	Information not held	0	0	0	0	Gov CertUK	0	Face-to-face training - additional guidance via online questionnaire, PowerPoint slides, ICO video, simulated phishing attacks and newsletter	All staff	6-7% of IT budget	Not stated
Newark and Sherwood		1	0	0	0	n/a	0	No specific training - part of Information Governance training	All staff	No specific budget allocated	No specific budget allocated

Mansfield	4	1	2	2	0	n/a	1	Mandatory training at induction and annual training - additional guidance and alerts	All staff	No specific budget allocated	In-house - no extra costs
Bassetlaw	Failed to reply to FOI										
Nottingham	Information not held	0	0	0	0	n/a	0	Mandatory training at induction	All staff	No specific budget allocated	In-house - no extra costs
City of London	Information not held	1	0	0	0	n/a	0	No training - in the process of rolling out	Unknown	Information not held	Information not held
Barking and Dagenham	Refused: Section 31(2) Prejudicial to Law Enforcement										
Barnet	Refused: Section 31(2) Prejudicial to Law Enforcement										
Bexley	Refused: Section 31(2) Prejudicial to Law Enforcement										
Brent	Refused: Section 17 and Section 31(2) Prejudicial to Law Enforcement										
Bromley	2	2	0	0	0	n/a	0	No training – part of Information Governance training	None	No specific budget allocated	No specific budget allocated
Camden	Refused: Section 31(2) Prejudicial to Law Enforcement										
Croydon	Information not held	2	0	0	0	n/a	0	Mandatory training part of Information Management	N/A	Service outsourced	n/a
Ealing	0	0	0	0	0	n/a	0	N/A	3,300	Not stated	Not stated
Enfield	Refused: Section 31(2) Prejudicial to Law Enforcement										
Greenwich	Refused: Section 31(2) Prejudicial to Law Enforcement										
Hackney	Refused: Section 31(2) Prejudicial to Law Enforcement							E-learning - additional information via intranet and internal communications	628	No specific budget allocated	No specific budget

											allocated
Hammersmith and Fulham	Information not held	1	0	0	0	n/a	1	E-learning - additional guidance via posters and service desk communications	All staff	No specific budget allocated	No specific budget allocated
Haringey	Refused: Section 31(2) Prejudicial to Law Enforcement										
Harrow	2	2	0	0	0	n/a	0	Mandatory training	All staff	Service outsourced	In-house - no extra costs
Havering	0	0	0	0	0	n/a	0	E-learning	All staff	No specific budget allocated	In-house - no extra costs
Hillingdon	Information not held	n/a	0	0	0	n/a	0	Training part of data protection training	All staff	No specific budget allocated	No extra costs - delivered in-house
Hounslow	Refused: Section 31(2) Prejudicial to Law Enforcement	0	0	0	0	n/a	0	No specific training - guidance via online, classroom and staff bulletins	All staff	No specific budget allocated	In-house - no extra costs
Islington	Information not held	1	1	1	0	n/a	0	E-learning - additional guidance via internal memos and intranet	All staff (approx.4000)	No specific budget allocated	No specific budget alloca

											ted
Kensington and Chelsea	Refused: Section 31(2) Prejudicial to Law Enforcement							No training - guidance via intranet and emails	All staff	No specific budget allocated	No specific budget allocated
Kingston upon Thames	0	0	0	0	0	n/a	0	Refused: Section 31(2) Prejudicial to Law Enforcement		No specific budget allocated	No specific budget allocated
Lambeth	3	3	0	0	0	n/a	1	No training - guidance via intranet	Information not held	Information not held	Information not held
Lewisham	Refused: Section 31(2) Prejudicial to Law Enforcement										
Merton	6	6	0	0	0	n/a	3	Annual e-learning	1747	6%	No extra cost
Newham	0	0	0	0	0	n/a	0	E-learning - part of data protection training	All staff	No specific budget allocated	No specific budget allocated
Redbridge	Unquantifiable	3	0	0	0	n/a	0	Mandatory training at induction - additional annual refresher courses	All staff	Information not held in requested format	Information not held in requested format

Richmond upon Thames	8	5	0	0	0	n/a	0	Mandatory e-learning - part of Information Governance and Data Protection, refreshed bi-annually	786	3%	3%
Southwark	0	0	0	0	0	n/a	0	E-learning - part of Information Governance training	1444	Information not held	No extra costs - delivered in-house
Sutton	0	0	0	0	0	n/a	0	Refused: Section 31(2) Prejudicial to Law Enforcement		Information not held in requested format	Information not held in requested format
Tower Hamlets	0	0	0	0	0	n/a	0	No training - guidance via intranet	Information not held	No specific budget allocated	No specific budget allocated
Waltham Forest	Refused: Section 31(2) Prejudicial to Law Enforcement										
Wandsworth	5	2	0	0	0	n/a	0	Mandatory e-learning - part of Information Security, refreshed bi-annually	3538	Information not held	Information not held
Westminster	3	3	1	0	0	n/a	3	No training - guidance via intranet and emails	All staff	service outsourced	n/a
North Lincolnshire	Refused: Section 31(2) Prejudicial to Law Enforcement										
North East Lincolnshire	Refused: Section 31(2) Prejudicial to Law Enforcement										

East Riding of Yorkshire	Information not held	Information not held	Information not held	Information not held	Information not held	Information not held	Information not held	In the process of rolling out training	Not stated	Information not held in requested format	Information not held in requested format
Kingston upon Hull	Unquantifiable	3	3	3	0	n/a	0	Support provided no details of training	All staff	Information not held in requested format	Information not held in requested format
Leeds	Log not kept	number not specified	0	0	0	0	0	Mandatory periodic survey including tests - additional guidance via security policies, intranet, newsletters, briefings and e-bulletins	All staff	1.2%	Not stated
Wakefield	Unquantifiable	0	0	0	0	n/a	0	Mandatory annual e-learning - additional guidance via intranet, e-bulletins	2223	No specific budget allocated	Information not held
Kirklees	2	number not specified	0	0	0	1 CertUK	0	E-learning - additional training via phishing simulations	All staff	2% of overall IT budget	within 2% of overall IT budget
Calderdale	0	1	0	0	0	n/a	0	Annual e-learning part of Information security training, additional guidance via newsletters, emails, bulletins and PowerPoints	All staff	Information not held in requested format	No specific budget allocated
Bradford	Failed to reply to FOI										

High Peak	0	0	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated
Sheffield	2	1	0	0	0	n/a	0	Training part of Protecting Information and Data Protection courses - additional guidance via briefings and posters	Protecting Information course: 1643; Data Protection course: 2095	Information not held in requested format	Information not held in requested format
Rotherham	1	0	1	0	0	n/a	0	E-learning	All ICT users	Information not held	No specific budget allocated
Doncaster	1	1	0	0	0	1 Gov CertUK, Y&HWARP	0	Mandatory e-learning - refreshed every 3 years	Approx. 400	Information not held	Information not held
Barnsley	1	1	0	0	0	n/a	0	Annual training - additional guidance via intranet and newsletters	All ICT users	2.7%	Minimal costs - delivered in house
North Yorkshire County Council	Refused: Section 31(2) Prejudicial to Law Enforcement										
Selby	Information not held	0	0	0	0	n/a	0	No training - guidance via intranet	0	6%	0
Harrogate	0	0	0	0	0	n/a	0	Mandatory e-learning on ICT User Policy	513	No specific budget allocated	No specific budget allocated

Craven	Refused: Section 31(2) Prejudicial to Law Enforcement							Training part of data protection training	Not stated	Information not held - partly outsourced	Information not held - partly outsourced
Richmondshire	0	0	0	0	0	n/a	0	E-learning	All ICT users + 2 specialists	6%	2%
Hambleton	Refused: Section 31(2) Prejudicial to Law Enforcement										
Ryedale	0	0	0	0	0	n/a	0	No specific training - part of Data Protection and Information management framework	All staff	No specific budget allocated	No specific budget allocated
Scarborough	0	0	0	0	0	n/a	0	E-learning - additional guidance via emails and bulletins	All staff	6.89%	1.08 %
York	Information not held	0	0	0	0	n/a	0	E-learning and face to face training	All ICT users	2%	0.50 %
Redcar and Cleveland	Refused: Section 31(2) Prejudicial to Law Enforcement										
Gateshead	65,000 per month	1	0	0	0	n/a	0	No specific training - data protection training only and additional guidance via ICT policy and briefings	All staff	No specific budget allocated	No specific budget allocated
Northumberland	Refused: Section 31(2) Prejudicial to Law Enforcement										
Newcastle-upon-Tyne	Refused: Section 31(2) Prejudicial to Law Enforcement							E-learning - additional guidance via intranet and emails	All staff	No specific budget allocated	No specific budget allocated

North Tyneside	3	0	0	0	0	n/a	0	Training part of Information governance and security training at induction - regular refresher courses	78.86%	16%	No extra costs - delivered in-house
South Tyneside	Records not held	Records not held	Records not held	Records not held	Records not held	Records not held	Records not held	No training - guidance via email only	n/a	Refused: Section 43 Commercial interests	Refused: Section 43 Commercial interests
Sunderland	Refused: Section 31(2) Prejudicial to Law Enforcement							No training - guidance via regular briefings	Refused: Section 31(2) Prejudicial to Law Enforcement		
Durham	approx 1.3 million per month	0	0	0	0	n/a	0	Training - additional guidance via intranet, security events, phishing simulations and update training	6,500	>1%	>1%
Hartlepool	2	0	1	0	0	n/a	0	No training - guidance via email campaigns	All staff	Service outsourced	0
Darlington	Records not held	0	0	0	0	n/a	0	E-learning - refresher course every 2-3 year, updates and alerts	All staff	Information not held in requested format	Information not held in requested format
Stockton-on-Tees	Refused: Section 31(2) Prejudicial to Law Enforcement										
Middlesbrough	Refused: Section 31(2) Prejudicial to Law Enforcement									approx. £90k	0
Cumbria	0	0	0	0	0	n/a	0	Mandatory annual training - part of Information Security awareness	5,000	6%	Not stated

Barrow-in-Furness	12	4	0	0	0	n/a	0	No specific training - part of Information Security Awareness training	All staff	Information not held	Information not held
South Lakeland	0	0	0	0	0	n/a	0	Training at induction - part of general data protection training	All staff	Not held in requested format	Not held in requested format
Copeland	0	0	0	0	0	n/a	0	None	5	0%	0%
Allerdale	0	0	0	0	0	n/a	0	No training - guidance via intranet and mandatory ICT security policy	Information not held	No specific budget allocated	No specific budget allocated
Eden	0	0	0	0	0	n/a	0	No specific training - part of general data protection training	All staff	No specific budget allocated	No specific budget allocated
Carlisle	0	0	0	0	0	n/a	0	No specific training - part of Ethical Governance Programme	30	0.46%	No specific budget allocated - training delivered in-house

Lancashire	2	2	0	0	0	n/a	0	Mandatory e-learning	5,000	service outsourced - information commercially confidential	Not stated
West Lancashire	3	3	0	0	0	n/a	0	No specific training	20	service outsourced - information commercially confidential	n/a
South Ribble	0	0	0	0	0	n/a	0	Ad hoc training - additional guidance through updates and security policy	All staff	Approx. 30% of ICT budget	No extra cost
Chorley	2	1	0	0	0	n/a	0	Mandatory e-learning at induction	All staff	Less than 1% of overall annual budget	Less than 1% of overall annual budget
Fylde	1	1	0	0	0	n/a	0	Mandatory e-learning	All staff	No specific budget allocated	No specific budget allocated
Preston	Refused: Section 31(2) Prejudicial to Law Enforcement										
Wyre	Refused: Section 31(2) Prejudicial to Law Enforcement										
Lancaster	Refused: Section 31(2) Prejudicial to Law Enforcement							Mandatory e-learning part of Information Governance and Data Protection training	Not stated	No specific budget allocated	No specific budget allocated
Ribble Valley	Failed to reply to FOI										
Pendle	IT outsourced										

Burnley	2	2	0	0	0	n/a	0	Not stated	Not stated	service outsourced - information commercially confidential	Not stated
Rossendale	Refused: Section 31(2) Prejudicial to Law Enforcement										
Hyndburn	2	2	0	0	0	n/a	0	Training at induction - additional guidance via updates/reminders and internal communication	All staff	No specific budget allocated	No specific budget allocated
Blackpool	1	1	0	0	0	n/a	1	No formal training - guidance via intranet	20 specialists	2013-2015 approx. 2%, 2016-2017 5%	No extra cost - delivered in-house
Blackburn with Darwen	Refused: Section 31(2) Prejudicial to Law Enforcement										
Warrington	1	1	0	0	0	n/a	0	No specific training - part of Information security training with additional guidance on intranet	Not stated	No specific budget allocated	No specific budget allocated
Manchester	Refused: Section 31(2) Prejudicial to Law Enforcement										
Stockport	Refused: Section 31(2) Prejudicial to Law Enforcement										
Tameside	Records not held	Records not held	n/a	n/a	n/a	n/a	n/a	E-learning - part of Information Governance Framework	All ICT users	No information held in requested format	No information held in requested format

Oldham	0	0	0	0	0	n/a	0	Training part of Data protection and Information Security training - additional guidance via briefings and internal communications	All ICT staff	Refused: Section 43 Commercial interests	Refused: Section 43 Commercial interests
Rochdale	Refused: Section 24 National Security and Section 31(2) Prejudicial to Law Enforcement										
Bury	0	0	0	0	0	n/a	0	No training - Information security policy only	All staff	11.5% of ICT budget	Information not held
Bolton	Refused: Section 31(2) Prejudicial to Law Enforcement								All staff	Information not held in requested format	Information not held in requested format
Wigan	Refused: Section 31(2) Prejudicial to Law Enforcement										
Salford	Refused: Section 31(2) Prejudicial to Law Enforcement										
Trafford	Refused: Section 31(2) Prejudicial to Law Enforcement							Mandatory e-learning at induction	2553	0.04% of Council's budget	No specific budget allocated
Halton	Refused: Section 31(2) Prejudicial to Law Enforcement										
Liverpool	Information not held	1	0	0	0	1 CiSP	0	Only ICT staff required to take annual security training and data protection training	409	2%	0%
Sefton	Refused: Section 31(2) Prejudicial to Law Enforcement										
Knowsley	0	0	0	0	0	n/a	0	Mandatory annual training - part of Information Security week	All ICT users	7.75% of ICT budget	included in 7.75 ICT

											budget
St. Helens	1	0	0	0	0	n/a	0	Training - part of Information Management Framework	All staff	13% of ICT budget	No extra costs - delivered in-house
Wirral	Refused: Section 31(2) Prejudicial to Law Enforcement								All ICT users	No specific budget allocated	No specific budget allocated
Oxfordshire County Council	2	0	0	0	0	n/a	0	Cyber security awareness week - additional guidance via intranet	Not stated	Information can't be calculated	Information can't be calculated
Oxford	Refused: Section 31(2) Prejudicial to Law Enforcement										
Cherwell	2	2	0	0	0	n/a	0	Mandatory e-learning at induction - additional guidance vial emails	All staff	No specific budget allocated	No specific budget allocated
Vale of White Horse	0	0	0	0	0	n/a	0	E-learning - additional guidance via keep safe tips	Not stated	Service outsourced	Service outsourced
West Oxfordshire	9000	0	0	0	0	n/a	0	No training - Online guidance and keep safe tips	Not stated	No specific budget allocated	No specific budget

											allocated
Reading	0	0	0	0	0	n/a	0	Not stated	All staff	Services outsourced	Services outsourced
Wokingham	0	0	0	0	0	n/a	0	n/a	6	£50K	n/a
Bracknell Forest	Refused: Section 31(2) Prejudicial to Law Enforcement										
Windsor and Maidenhead	Refused: Section 24 National Security										
Slough	8	8	0	0	0	n/a	0	E-learning	Not stated	Service outsourced	No specific budget allocated
South Oxfordshire	See response Vale of White Horse										
Hart	Refused: Section 31(2) Prejudicial to Law Enforcement										
Rushmoor	0	0	0	0	0	n/a	0	Annual e-learning	All staff	No specific budget allocated	No specific budget allocated
Basingstoke and Deane	0	0	0	0	0	n/a	0	E-learning part of Data Protection and Anti-fraud training - additional guidance via emails and phishing training software	All staff	approx. 10%	approx. 10%
Hampshire	Information not held	2	0	1	0	n/a	1	Mandatory e-learning at induction	96% of staff	No specific budget allocated	No specific budget allocated
Gosport	Failed to reply to FOI										

Fareham	Refused: Section 31(2) Prejudicial to Law Enforcement							Mandatory training at induction - additional guidance bulletins on intranet	Approx. 500	No specific budget allocated	No specific budget allocated
Winchester	0	0	0	0	0	n/a	0	Training at induction - additional guidance via IMT security conduct & policy and staff bulletin	All staff	2013: 27k – 14% 2014: 38k - 19% 2015: 42k - 21% 2016: 45K – 24%	2013: 0% 2014: 0.7% 2015: 0.6% 2016: 2.6%
Havant	0	0	0	0	0	n/a	0	No training - Online guidance and keep safe tips	Not stated	No specific budget allocated	No specific budget allocated
East Hampshire	0	0	0	0	0	n/a	0	No training - guidance via general communication on regular basis	7 specialists	No specific budget allocated	No specific budget allocated
Test Valley	0	0	0	0	0	n/a	0	No training - signing of Information Security and GCSX Email Acceptable Usage Policy at induction	All staff	5.64% of IT budget	No specific budget allocated
Eastleigh	2	2	0	0	0	n/a	0	No formal training - guidance via ad hoc bulletin and online video	1 specialist	15%	No specific budget allocated

New Forest	1	1	0	0	0	n/a	0	E-learning at induction - annual refresher courses	All staff	1%	<1%
Southampton	2	2	0	0	0	n/a	0	Information not held	Information not held	Service outsourced	Service outsourced
Isle of Wight	Records not held - not holding incident log							Mandatory training part of Information Security and Data Protection training	All staff	2.5% of annual ICT budget	0.01 % of ICT budget
Portsmouth	463,000	4	0	0	0	n/a	0	Training part of Security and Information Governance training at induction - additional guidance via annual refresher courses and intranet	All staff	1% of annual ICT budget	0.25 % of ICT budget
Dorset	Failed to reply to FOI										
Weymouth and Portland	0	0	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated
West Dorset	0	0	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated
North Dorset	4	4	Refused: Section 31(2) Prejudicial to Law Enforcement				0	Training part of induction	150	Now provided by West Dorset Council	Now provided by West Dorset Council
Purbeck	8164	1	1	0	4	n/a	0	Regular sessions at briefings - additional guidance via articles, intranet and emails	All staff	2016/17: 5%	2016/17: 13%
East Dorset	0	0	0	0	0	n/a	0	E-learning	All staff	4%	Not stated
Christchurch	See response East Dorset										

Bournemouth	0	0	0	0	0	n/a	0	Mandatory face-to-face training part of Information Security training. Refresher course every 3 years.	23	No specific budget allocated	No specific budget allocated
Poole	2	2	1	0	0	n/a	0	Mandatory e-learning at induction - additional guidance via intranet	601	No specific budget allocated	£10500 on e-learning in general
Kent County Council	3	3	1	1	1	n/a	0	E-learning - part of cyber crime, cyber security and cyber crime phishing training	Cyber Crime: 314 Cyber Security: 223 Cyber Crime Phishing: 254	£401,585.82	No extra costs - delivered in-house
Sevenoaks	0	0	0	0	0	n/a	0	No training	2 specialists	2% Firewalls & AV Products	0%
Dartford	0	0	0	0	0	n/a	0	No training - guidance via emails only	All staff	Information not held in requested format	No specific budget allocated
Gravesham	0	0	0	0	0	n/a	0	Training part of Data Protection training	All staff	2.4% of annual IT budget	No specific budget allocated

Tonbridge and Malling	0	62	0	1	0	n/a	2	E-learning in the process of being rolled out - currently guidance via alerts and Information Security Policy agreement	All staff	No specific budget allocated	No specific budget allocated
Medway	Failed to reply to FOI										
Maidstone	0	0	0	0	0	n/a	0	No details given	Not stated	25-35%	0%
Tunbridge Wells	0	0	n/a	n/a	n/a	n/a	0	No details given	Not stated	25-35%	0%
Swale	0	0	0	0	0	n/a	0	No details given	Not stated	25-35%	0%
Ashford	IT outsourced		0	0	0	n/a	0	Mandatory annual e-learning	All staff	5%	Information not held
Canterbury	12	0	0	0	0	n/a	2	No specific training	n/a	No specific budget allocated	No specific budget allocated
Shepway	Information not held	0	0	0	0	n/a	0	No training - Awareness raised through "Use of computers" policy at induction and quarterly email reminders	Not stated	Service outsourced	
Thanet	Refused: Section 31(2) Prejudicial to Law Enforcement										
Dover	10	0	0	0	0	n/a	0	No training - Information Governance policy renewed January 2017 additional guidance via email campaign	All staff	Information not held in requested format	Information not held in requested format
Surrey County Council	2	2	0	0	0	n/a	0	IT Security Learning package	1527	1% of It budget	Minimal

Spelthorne	0	0	0	0	0	n/a	0	Internal training - no further details	All staff	5%	No extra costs - delivered in-house
Runnymede	0	0	0	0	0	n/a	0	No details given	500	2.50%	No extra costs - delivered in-house
Surrey Heath	Refused: Section 31(2) Prejudicial to Law Enforcement							Annual training part of Data Protection training	All staff	Information not held in requested format	Information not held in requested format
Woking	0	0	0	0	0	n/a	0	Mandatory training at induction - additional guidance via intranet , posters and security policy agreement	All staff	No specific budget allocated	No specific budget allocated
Elmbridge	0	0	0	0	0	n/a	0	Mandatory annual training	All staff	approx. 10%	No specific budget allocated

Guildford	0	0	0	0	0	n/a	0	Training part of data protection training - additional guidance via emails	All staff	No specific budget allocated	No specific budget allocated
Waverley	0	0	0	0	0	n/a	0	Mandatory e-learning at induction	All staff	Information not held in requested format	Information not held in requested format
Mole Valley	5	4	1	1	0	n/a	0	Mandatory training and awareness testing - additional monthly phishing test	All staff	Information not held in requested format	~0.002%
Epsom and Ewell	0	0	0	0	0	n/a	0	Training provided in-house	All staff	Not stated	Not stated
Reigate and Banstead	1	1	0	0	0	n/a	0	Mandatory e-learning at induction	All staff	No specific budget allocated	No specific budget allocated
Tandridge	1	1	0	0	1	n/a	0	No training - guidance via updates and messages on intranet	1 specialist	3.70%	<1%
East Sussex	Refused: Section 31(2) Prejudicial to Law Enforcement							Mandatory training part of Information security training - additional guidance via articles and briefs	All staff	2012/13 – 0.06%; 2013/14 - 0.2%; 2014/15 – 0.1%; 2015/16 – 0.2%; 2016/17 – 0.02%.	No extra costs - delivered in-house

Hastings	Refused: Section 31(2) Prejudicial to Law Enforcement										
Rother	0	0	0	0	0	n/a	0	Basic awareness session	All staff	No set ICT budget	No specific budget allocated
Wealden	2	2	0	0	0	n/a	0	No specific training - part of mandatory yearly Data Protection Awareness	All staff (360)	Information not held in requested format	No specific budget allocated
Eastbourne	See response Lewes										
Lewes	Refused: Section 31(2) Prejudicial to Law Enforcement and Section 43 Prejudicial to commercial interests										
Brighton & Hove	Refused: Section 31(2) Prejudicial to Law Enforcement and Section 43 Prejudicial to commercial interests							No specific training - part of Information Governance training - guidance via email	All staff	Information not held	Information not held
West Sussex County Council	Refused: Section 31(2) Prejudicial to Law Enforcement							Mandatory training at induction and annual training	All staff	No specific budget allocated	No specific budget allocated
Worthing	See response Adur										
Arun	Refused: Section 31(2) Prejudicial to Law Enforcement										
Chichester	751	0	0	0	0	n/a	0	Training at induction - regular refresher courses, additional guidance via intranet and updates	All staff	15%	No specific budget allocated
Horsham	0	0	0	0	0	n/a	0	No training	0	No specific budget allocated	n/a

Crawley	0	Information not held	0	0	0	n/a	0	e-learning - additional guidance via intranet	2013: 212 2014: 30 2015: 44 2016: 79 2017: 25	Information not held	No specific budget allocated
Mid Sussex	2	2	0	2	0	n/a	0	No training	None	£39,000	n/a
Adur	0	0	0	0	0	n/a	0	No training - guidance via intranet and bulletins	No information held	0	0
West Berkshire	3	0	0	0	0	n/a	0	Mandatory face to face training	All staff	0.05%	Not stated
Cornwall	0	0	0	0	0	n/a	0	Non-mandatory e-learning - additional guidance via updates and warnings of cyber attacks	Approx. 1000	No specific budget allocated	No specific budget allocated
Isles of Scilly	0	0	0	0	0	n/a	0	n/a	0	n/a	n/a
Devon	Information not held	0	0	0	0	0	0	Training part of mandatory Data Protection e-learning	All staff	2013 – 2014: 0.011% 2014 – 2015: 0.012% 2015 – 2016: 0.014% 2016 – 2017: 0.011%	No specific budget allocated
Exeter	2	0	0	0	0	n/a	0	Annual training part of Security Awareness training	600	No specific budget allocated	No specific budget allocated
East Devon	0	0	0	0	0	n/a	0	Training part of annual Information Security training	Approx. 500	No specific budget allocated	No specific budg

											et allocated
Mid Devon	Refused: Section 31(2) Prejudicial to Law Enforcement										
North Devon	Information not held	0	0	0	0	n/a	0	No training	None	3%	No specific budget allocated
Torridge	Unquantifiable	0	0	0	0	n/a	0	Training part of Email Virus Awareness	All staff	No specific budget allocated	No extra costs - delivered in-house
West Devon	Failed to reply to FOI										
South Hams	Failed to reply to FOI										
Teignbridge	IT services outsourced to Strata Service Solutions Ltd										
Plymouth	Refused: Section 31(2) Prejudicial to Law Enforcement										
Torbay	3	3	0	0	0	n/a	0	Mandatory e-learning - additional guidance via intranet	683 (2013); 99 (2014); 154 (2015); 198 (2016); 82 (2017 to date)	2013/2014 £74,100; 2014/2015 £75,220; 2015/16 £56,436; 2016/17 £129.211; 2017/18 £26,969	0
Bristol	Refused: Section 31(2) Prejudicial to Law Enforcement										
Bath and North East Somerset	0	0	0	0	0	n/a	0	In the process of rolling out training - guidance via intranet and emails	Cyber Security e-Learning is not yet live	3.8% of annual IT budget	Cyber Security e-Learning is not

											yet live
North Somerset	1	1	Not stated	Not stated	Not stated	Not stated	Not stated	Mandatory training part of Information Security and Secure Email training	1878	Service outsourced	No specific budget allocated
Gloucestershire	0	0	0	0	0	n/a	0	Some staff were trained at the NCSC, All staff receive periodical emails advising them on actions. Also ad-hoc emails to inform about current threats	3 specialists	Service outsourced	No specific budget allocated
Gloucester	Exact figure not held	1	0	1	0	n/a	1	E-learning - additional guidance via bulletins and emails	All staff	service outsourced	Not stated
Cheltenham	approx 9000	0	0	0	0	n/a	0	Training provided in response to risk identified	All staff	35% of IT infrastructure costs	No specific budget allocated
South Gloucestershire	Refused: Section 31(2) Prejudicial to Law Enforcement							Mandatory training - additional guidance via presentations and interactive discussions	2000	Refused: Section 31(2) Prejudicial to Law Enforcement	
Tewkesbury	0	0	0	0	0	n/a	0	In the process of being rolled out	Not stated	No specific budget allocated	No specific budget allocated

Cotswold	approx 9000	0	0	0	0	n/a	0	Training provided in response to risk identified	All staff	35% of IT infrastructure costs	No specific budget allocated
Stroud	Refused: Section 12 Cost and time										
Somerset	30,000 per month	2	1	1	0	n/a	0	Mandatory e-learning at induction - additional guidance via periodic reminders	99.5% of staff	£250k - 300k	£10-15k
Forest of Dean	See response Cotswold										
South Somerset	0	0	0	0	0	n/a	0	Training and testing provided	ca. 500	Information not held	0.5%
Taunton Deane	2	0	0	0	0	n/a	1	No training - guidelines provided at induction	Not stated	approx. 45000	0
West Somerset	Failed to reply to FOI										
Sedgemoor	11	0	0	0	0	n/a	0	Training at induction	365 (all staff)	Information not held in requested format	No extra costs - delivered in-house
Mendip	1	1	0	0	0	n/a	1	Training at induction - additional guidance via intranet and weekly bulletin	All staff	No specific budget allocated	No specific budget allocated
Wiltshire	2	0	0	0	1	0	1	No training - information security training only	Information not held	Information not held in requested format	Information not held in requested

											format
Swindon	0	5	0	0	0	n/a	0	Training and testing via compliance pop-up tool	Not stated	Information not held in requested format	£11,695
Warwickshire	Refused: Section 31(2) Prejudicial to Law Enforcement										
Nuneaton and Bedworth	0	0	0	0	0	n/a	0	In the process of rolling out training	Not stated	No specific budget allocated	No specific budget allocated
Rugby	0	0	0	0	0	n/a	0	Training -part of Information Security, Data Protection and Employee Conduct.	All ICT users	Not stated	Not stated
Stratford-on-Avon	0	0	0	0	0	n/a	0	No training - general information provided	IT staff only	No specific budget allocated	No specific budget allocated
Warwick	Information not held	2	0	0	0	n/a	2	E-learning at induction - additional guidance via intranet	All staff	15.18%	0%
Herefordshire	27	22	2	0	0	n/a	0	Annual e-learning - additional guidance via bulletins, spoof phishing campaign	2015: 1155, 2016: 1342, 2017: 534	Information not held in requested format	Information not held in requested format
Worcestershire	Unknown	2	0	0	0	1 CertUK	0	In the process of rolling out training - currently guidance via intranet and emails	n/a	3.7% of ICT budget	Information not held

											in requested format
Worcester	1	1	0	0	0	n/a	0	Mandatory e-learning	All staff	<1% of ICT budget	<1% of ICT budget
Malvern Hills	0	0	0	0	0	n/a	0	Mandatory e-learning	All staff	<1% of ICT budget	<1% of ICT budget
Bromsgrove	Information not held										
Redditch	Information not held										
Wychavon	0	0	0	0	0	n/a	0	Mandatory e-learning	All staff	<1% of ICT budget	<1% of ICT budget
Telford & Wrekin	Refused: Section 38 Health and Safety										
Newcastle-under-Lyme	7	0	0	0	0	1 Action Fraud	0	Bi-annual training and training at induction	All staff	0.165% of £13.8m	0.144% of 13.8m
Staffordshire	Failed to reply to FOI										
Tamworth	1	1	0	0	0	n/a	0	E-learning	All staff	Information not held	Information not held
Staffordshire Moorlands	0	0	0	0	0	n/a	Not stated	Not stated	Not stated	Not stated	Not stated
Stafford	Refused: Section 31(2) Prejudicial to Law Enforcement, Section 43 Commercial Interests of the Council										
Cannock Chase	0	0	0	0	0	n/a	0	Training -part of ICT Security and policy awareness training	All staff	Not recorded	Not separately recorded
Lichfield	Refused: Section 31(2) Prejudicial to Law Enforcement										
Stoke-on-Trent	Refused: Section 31(2) Prejudicial to Law Enforcement, Section 24(1) National Security, Section 38(1) Health and Safety										

Shropshire	Refused: Section 31(2) Prejudicial to Law Enforcement							Annual mandatory e-learning	All staff	No specific budget allocated	No specific budget allocated
Cheshire West and Chester	Refused: Section 31(2) Prejudicial to Law Enforcement										
Cheshire East	Refused: Section 31(2) Prejudicial to Law Enforcement									Information not held	Refused: Section 31(2) Prejudicial to Law Enforcement
South Staffordshire	Failed to reply to FOI										
Wolverhampton	0	0	0	0	0	n/a	n/a	Annual training	All staff	No specific budget allocated	No specific budget allocated
Dudley	Refused: Section 31(2) Prejudicial to Law Enforcement							Mandatory annual e-learning - additional guidance via intranet	All staff	Refused: Section 31(2) Prejudicial to Law Enforcement	
Walsall	Failed to reply to FOI										
Sandwell	0	0	0	0	0	n/a	0	Cyber Response Incident Workshop	9	7%	7%
Birmingham	4	2	Not stated								
Solihull	Refused: Section 31(2) Prejudicial to Law Enforcement										
Coventry	Refused: Section 31(2) Prejudicial to Law Enforcement										

Wyre Forest	5	5	0	0	0	n/a	0	In the process of being rolled out - currently guidance via intranet, online magazine, media screen and emails	All staff	Not identifiable - but budget has increased	Not stated
North Warwickshire	Failed to reply to FOI										
Aberdeen City	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Mandatory e-learning	All ICT users	Revenue Budget: 13/14: 0.02%, 14/15: 0.02%, 15/16: 0.03%, 16/17: 0.03%. Capital Budget 13/14, 14/15 & 15/6 0%, 16/17: 0.12%	0%
Aberdeenshire	1	0	0	0	0	n/a	0	No training - guidance via intranet	Information not held	Information not held	Information not held
Angus	Information not held In accessible format	Information not held In accessible format	0	0	0	n/a	0	Ongoing training - no details provided	Not stated	Information not held in requested format	Information not held in requested format
Argyll and Bute	1000s a day	1	0	0	0	n/a	0	Training at induction	Information not held	Information not held	Information not held
Clackmannanshire	29,000	3	Not stated	Not stated	Not stated	Not stated	0	E-learning part of Data Protection training - additional guidance via intranet	n/a	Not stated	Not stated
Dumfries and Galloway	Refused: Section 31(2) Prejudicial to Law Enforcement							No training	N/A	Information not held	Information not

											held
Dundee City	1000s a month	3	0	0	1	0	1	Refused: Section 31(2) Prejudicial to Law Enforcement			
East Ayrshire	Unquantifiable	0	0	0	0	n/a	0	Training to be launched September 2017	Not stated	No specific budget allocated	£1,000 for the course, £60 to upload.
East Dunbartonshire	3	3	0	0	0	n/a	0	Certified Security Manager, along with attendance at webinars/conferences in cyber security	1 specialist	6.9%	1%
East Lothian	11	0	0	1	0	n/a	0	Mandatory training at induction	Information not held	No specific budget allocated	No specific budget allocated
East Renfrewshire	2	2	0	0	0	n/a	0	E-learning part of Information Security & Privacy and Information Security	Unknown	8% of overall ICT budget	No specific budget allocated
City of Edinburgh	hundreds a day	11	0	1	0	n/a	1	E-learning - additional guidance via intranet, emails, poster and awareness campaigns	All staff	No specific budget allocated	No specific budget allocated
Eilean Siar	0	0	0	0	0	n/a	0	Training at induction - e-learning to be rolled out	All staff	5%	1%
Falkirk	Refused: Section 31(2) Prejudicial to Law Enforcement										

Fife	No records held	0	0	0	0	0	0	Training - part of data protection training, additional guidance via intranet, articles and testing of phishing awareness	11,500	No specific budget allocated	No specific budget allocated
Glasgow City	Refused: Section 31(2) Prejudicial to Law Enforcement							Mandatory e-learning	31,700	Refused: Section 31(2) Prejudicial to Law Enforcement	Information not held
Highland	952	0	0	0	0	n/a	0	No training	None	No specific budget allocated	None
Inverclyde	1	1	0	0	0	n/a	0	Mandatory training	32 (all staff)	No specific budget allocated	No specific budget allocated
Midlothian	2	0	1	0	0	1 GovCertUK	0	Training at induction - additional guidance via email, internal magazine	All staff	No specific budget allocated	No specific budget allocated
Moray	0	1	Not stated	Not stated	Not stated	Not stated	Not stated	No specific training - partly included in Data Protection training	Information not held	Information not held	Information not held
North Ayrshire	Refused: Section 31(2) Prejudicial to Law Enforcement							E-learning and face to face training- additional guidance via emails	2013 = 77 2014 = 216 2015 = 826 2016 = 1338 To 21st July 2017	8.0%	Information not held

									= 1291		
North Lanarkshire	Information not held	5	0	0	0	n/a	0	E-learning - additional guidance via intranet, email and posters	Not possible to identify number	Information not held	Information not held
Orkney	3	3	3	0	0	n/a	0	Refused under S30(c) FOI(S)A where disclosure of this information may harm the effective conduct of public affairs	All staff	No specific budget allocated	No extra costs - delivered in-house
Perth and Kinross	Not recorded	3	0	0	0	n/a	0	Mandatory e-learning - additional guidance via news alerts, blogs, briefings and posters	5819	Information not held in requested format	Information not held in requested format
Renfrewshire	Records not held	0	0	0	0	n/a	0	In the process of rolling out training	4825 members of staff and 2 specialists	5% of the overall ICT budget	£4,000
Scottish Borders	0	0	0	0	0	n/a	0	Mandatory e-learning	2872	Information not held	Information not held
Shetland	0	2	2	0	2	0	2	Penetration testing training	5	Not stated	No specific budget alloca

											ted
South Ayrshire	7	7	0	0	0	n/a	0	Mandatory e-learning - part of Data Protection Awareness and Information Security Awareness -additional guidance via bulletins, ICT awareness policy and posters	Data Protection Awareness : 1942, Information Security Awareness : 1496	No specific budget allocated	No specific budget allocated
South Lanarkshire	0	0	0	0	0	n/a	Refused: Section 17 does not retain all requested information				
Stirling	0	6	0	0	0	n/a	0	One member of staff trained in ethical hacking	All ICT staff	Information not held	No specific budget allocated
West Dunbartonshire	5	Details not disclosed for security reasons	1	0	0	1PSNA	0	Training at induction- rolling program of cyber security awareness sessions for existing staff	75% of ICT users	24.50%	No extra cost - delivered in-house
West Lothian	Failed to reply to FOI										
Blaenau Gwent	IT outsourced										
Bridgend	0	0	0	0	0	n/a	0	ICT staff only	N/A	No specific budget allocated	No specific budget allocated
Caerphilly	7	7	0	0	0	n/a	0	E-learning - additional guidance via email, posters, electronic pop-up advice and notifications	3,200	Information not held	Information not held

Cardiff	2	0	0	0	0	n/a	0	Training - additional guidance via policies, procedures and messages	All staff	Information not held in requested format	Information not held in requested format
Carmarthenshire	Information not held										
Ceredigion	Information not held	Information not held	0	0	0	n/a	0	Face to face training	967	No specific budget allocated	No specific budget allocated
Conwy	Information not held	1	0	0	0	n/a	1	Bi-annual training - additional guidance via email	All staff	No specific budget allocated	No specific budget allocated
Denbighshire	1	0	0	0	0	n/a	0	No training - "awareness communicated as and when necessary"	Information not held	Information not held	Information not held
Flintshire	Information not held	0	0	0	0	n/a	0	No specific training - part of IT induction and Data Protection training	Information not held	Information not held	No cost for this service
Gwynedd	2	0	0	0	0	n/a	0	No formal training - verbal training	All staff	No specific budget allocated	No specific budget allocated

Isle of Anglesey	0	0	0	0	0	n/a	0	Annual data protection training - additional guidance via email	All staff	No specific budget allocated	No specific budget allocated
Merthyr Tydfil	1	0	0	0	0	n/a	0	Annual e-learning	1200	30%	5.0%
Monmouthshire	15	Not stated	0	0	0	n/a	0	Training at induction and annual refresher courses	All staff	5.3%	0%
Neath Port Talbot	Failed to reply to FOI										
Newport	hundreds a day	1	1	0	0	n/a	0	Mandatory e-learning	1232	No specific budget allocated	No specific budget allocated
Pembrokeshire	3	3	0	1	0	n/a	0	No training - regular guidance via email	Not stated	No specific budget allocated	No specific budget allocated
Powys	Unquantifiable	0	0	0	0	n/a	0	Mandatory training at induction and refresher training every 3 years - additional guidance via emails and bulletins	2115	No specific budget allocated	Information not held
Rhondda, Cynon, Taff	18	18	0	1	0	CERT UK	0	E-learning - additional guidance via policies and bulletins	3602	£62,660	Not stated
Swansea	0	0	0	0	0	n/a	0	E-learning - additional guidance via email	All staff	No specific budget allocated	No specific budget allocated

The Vale of Glamorgan	0	1	0	0	0	Gov CertUK	0	Training at induction - additional guidance via bulletins	All staff	10%	10%
Torfaen	15	Not stated	0	0	0	n/a	0	Annual training	All staff	3%	0%
Wrexham	0	2	0	0	0	n/a	1	Regular alerts and bulletins	Information not held	Information not held	Information not held
Antrim and Newtownabbey	2	2	0	0	0	n/a	0	E-learning	approx. 600	12.5%	No specific budget allocated
Ards and North Down	0	0	0	0	0	n/a	0	No training - emails about current threats and ICT user agreement only	All ICT users	1-2%	0%
Armagh City, Banbridge and Craigavon	Failed to reply to FOI										
Belfast	Refused: Section 12 Cost and time										
Lisburn Castlereagh	2	2	1	0	0	n/a	0	Mandatory e-learning	All staff	No specific budget allocated	No specific budget allocated
Causeway Coast and Glens	0	0	0	0	0	n/a	0	Awareness presentation to Senior Management	2 ICT specialists	0.1% overall budget	0.1% overall budget
Derry City and Strabane	0	0	0	0	0	n/a	0	No training - emails about current threats only	0	30%	0%
Fermanagh and Omagh	3	3	0	0	0	Senior Management within	0	Training at induction - additional e-learning available to all staff	300	10%	0.5%

						Council					
Mid and East Antrim	0	0	0	0	0	n/a	0	In the process of rolling out training	N/A	2%	Included in overall IT budget
Mid-Ulster	9881	0	0	0	0	n/a	0	1/2 face to face training	approx. 500	No specific budget allocated	£10,000
Newry, Mourne and Down	1	1	0	0	0	n/a	1	No training - guidance via email	0	2.8%	0%