REDSCAN
A KROLL BUSINESS

A Redscan report

Disjointed and under-resourced: cyber security across UK councils

A Freedom of Information analysis

Contents

Disclaimer

Redscan, A Kroll Business, provides the information in this report for general purposes only. All information is provided in good faith; however, we make no representation or warranty of any kind, express or implied, regarding the accuracy, adequacy, validity, reliability, availability or completeness of any information.

1. Overview

1.1. Introduction

Their crucial role in ensuring access to vital services means UK councils have to process huge volumes of data and comply with strict regulatory requirements.

In the last 12 months, there have been numerous reports of data breaches at UK councils. One of the most high-profile was a ransomware attack on Hackney Council, which forced critical services to be shut down for several weeks. Redcar & Cleveland Borough Council also suffered a cyber-attack, leading to over 135,000 residents being unable to access important services.

Incidents like these demonstrate that whenever an organisation has valuable data, cybercriminals will attempt to steal it, regardless of the impact. With more council employees working remotely, and city and town centres becoming increasingly connected, the cyber security challenges facing councils are only set to grow in the future.

In May 2021, the National Cyber Security Centre (NCSC) issued a set of cyber security principles on connected places for local authorities, highlighting the potential for smart cities to be targeted by attackers.

Our FOI analysis of cyber security across UK councils

To understand the unique data and information security challenges facing councils, we submitted Freedom of Information (FOI) requests to all 398 county, district, city, borough and unitary councils in the UK. Our analysis is based on data pertaining to 2020 and 2019.

The results provide a snapshop into the state of cyber security across UK councils and shine a spotlight on councils’ preparedness to tackle current and emerging threats.

1.2. Key findings

Councils are highly suseptible to data breaches

- We estimate that UK councils reported over 700 data breaches to the Information Commissioner's Office (ICO) in 2020, a 10% decrease compared to 2019
- At least 10 councils had their operations disrupted due to a breach or ransomware
- One council reported 29 data breaches to the ICO in 2020

Council employees lack security training and qualifications

- Just over 50% of all UK council staff received cyber security training in 2020
- Nearly a third of councils reported that less than a quarter of staff had received training
- Forty-five percent of councils employ no professionals with recognised security qualifications

There are large disparities in security training spend

- The average annual spend on cyber security training by councils in 2020 was £3,343
- Annually, councils spend, on average, £1.58 on security training per employee
- Approximately four in ten councils spent no money on security training in 2020

2. The scale of data breaches

2.1. Total number of data breaches reported to the ICO

>700 breaches in 2020

Estimated number of data breaches reported to the ICO by UK councils

2 breaches per day

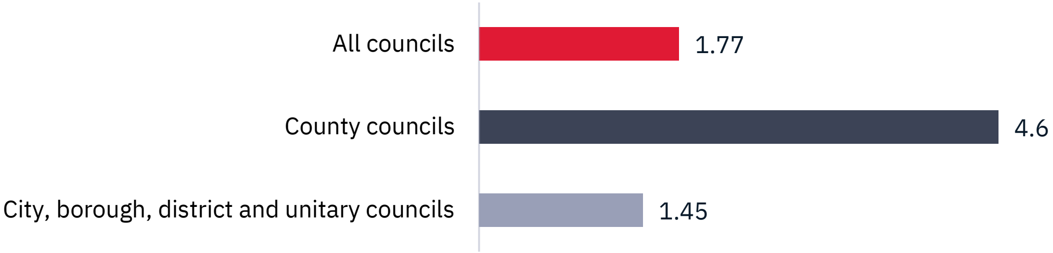
Total estimated number of data breaches reported daily to the ICO by UK councils in 2020

10 councils

Number of councils that reported data breaches or ransomware had disrupted public services in 2020

Data breaches occur for a variety of reasons, including human error and cyber incidents. The average number of data breaches reported by councils in 2020 was 1.77 per organisation. This is based on responses from nearly 250 councils. Extrapolating this figure across all 398 UK councils, we estimate that there were more than 700 data breaches reported by local authorities to the ICO in 2020. This equates to councils across the UK reporting in total almost two data breaches every day.

***Figure 1**: Average number of data breaches reported to the ICO by councils in 2020*



County councils experienced far more breaches than their city, borough, unitary and district counterparts, reporting 4.6 breaches on average to the ICO in 2020.

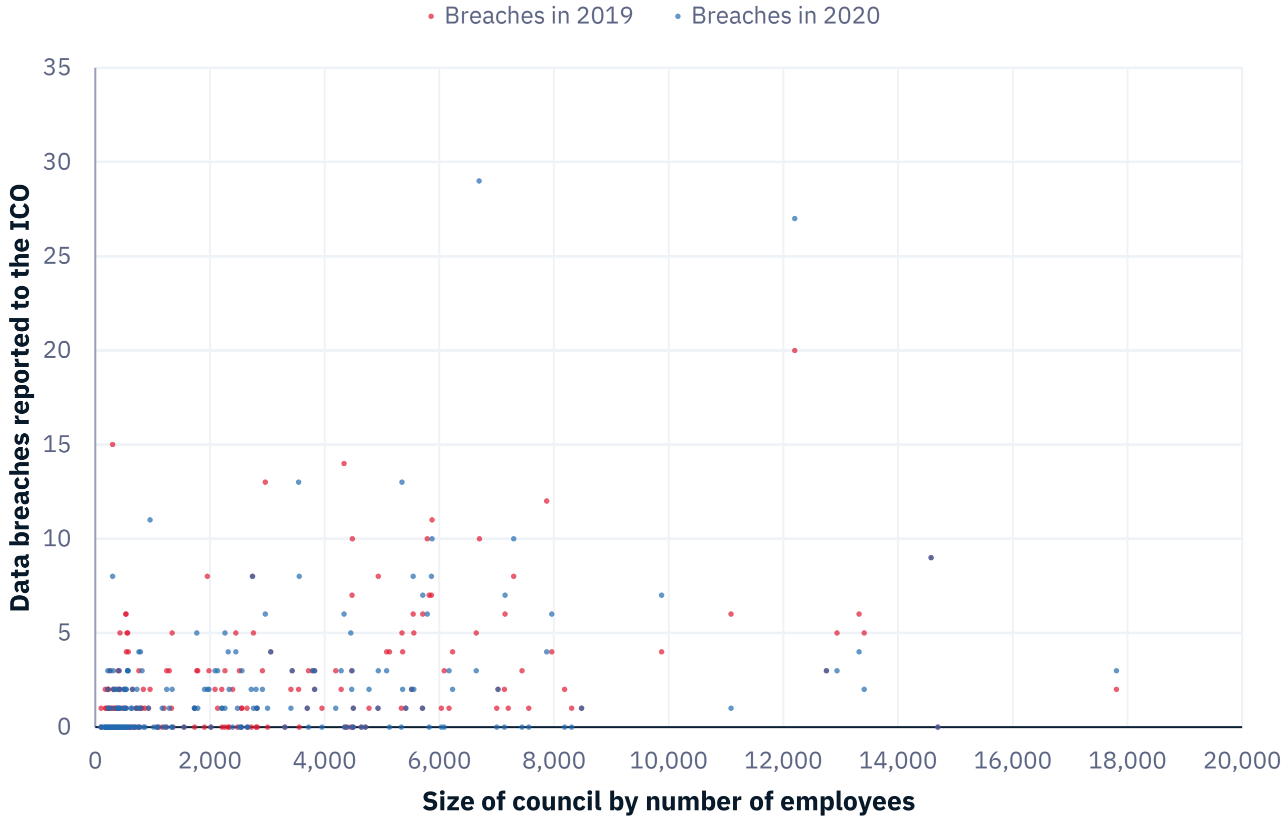
2.2. Data breach trends

Our analysis of data breach trends indicates that there is a strong correlation between council size and the number of breaches reported; councils reporting the most breaches were typically the largest.

The cluster at the bottom left of Figure 2 (councils with less than 2,000 employees) represents more than half of the councils that responded to our FOI request. This group reported, on average, 0.8 breaches to the ICO in 2020. In contrast, councils with more than 2,000 employees reported an average of 2.6 breaches during the same period.

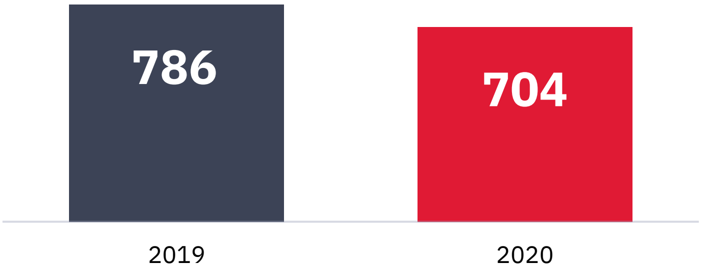
One city council with over 6,500 employees disclosed 29 breaches to the ICO in 2020 (compared to 10 in 2019), more than double the number reported by any other council in the UK. A council with just 300 employees reported 15 breaches in 2019 and a further eight in 2020.

***Figure 2**: Councils reporing data breaches to the ICO by council size*



Across the UK, we estimate that the total number of data breaches reported by councils to the ICO decreased between 2019 and 2020. In 2019, councils reported 1.98 breaches on average. Compared with 1.77 in 2020, this is a 10% year-on-year reduction. In terms of total breaches reported across the country, we estimate that this equates to a difference of about 80 breaches a year (786 vs. 704).

***Figure 3**: Estimated number of data breaches reported to the ICO by UK councils**



* Estimates based on an extrapolation of the responses received

Despite the estimated reduction in breaches since 2019, it is important not to underestimate the cyber security threat still faced by councils. As part of their responses to our FOI, ten councils confirmed that they were either a victim of ransomware or had experienced breaches that disrupted their operations. Of these councils, our research has found that only two incidents are in the public domain.[†]

What we say

“There are some pretty shocking data protection failings highlighted by our analysis, such as one council reporting 29 data breaches to the ICO in a single year.

“A notable number of councils experienced data breaches that impacted their ability to deliver important services. As towns and cities become more data-driven and interconnected, the possibilities for disruption will only increase. To minimise the risk of data breaches in the future, it is imperative that councils continually evaluate their security controls to keep up with the evolving threats.”

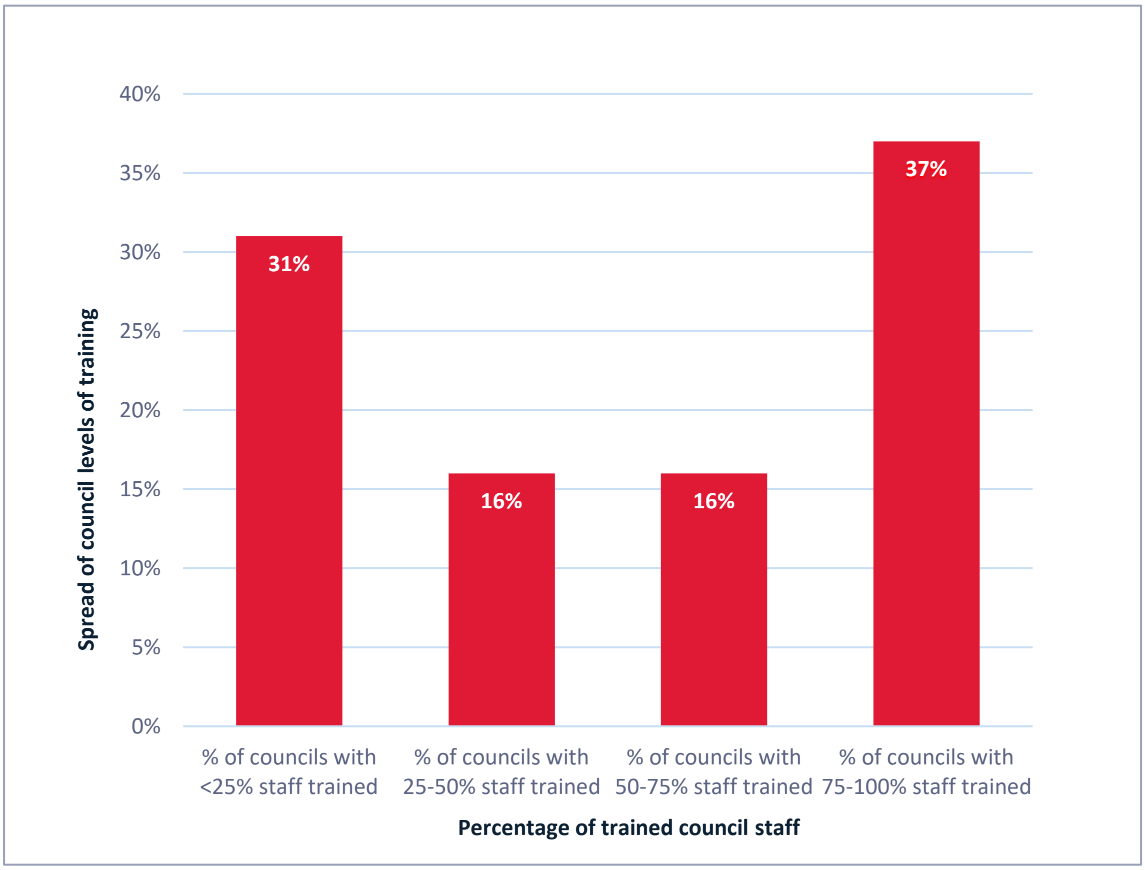
† Fifty councils declined to provide this data under Section 31 or other exemptions to the FOI Act so the figure could be even higher.

3. Employee security training

3.1. No common approach to training

Only half of employees across all UK councils received cyber security training in 2020 (53%). Nearly a third of councils (31%) reported that less than a quarter of their staff had received any cyber security training last year.

Figure 4: *Breakdown of councils by % of staff that received security training in 2020*



Attitudes to training vary considerably. Some councils said they have implemented policies to ensure all employees undertake cyber security training at least once a year. Others said they did not provide any training in 2020 or confirmed that only new employees, as part of their onboarding process, are required to complete security training. Some councils that did have formal security training processes reported that COVID-19 had disrupted their plans and, as a result, they had scaled them back.

3.2. Large disparities in training spend

£1.5m security spending

Total estimated amount spent on security training in 2020

£1.58 spend per person

The average security training spend per council employee in 2020 (across all UK councils)

Across the UK, we estimate that councils spent approximately £1.5 million on security training in 2020, which equates to £1.58 per employee. Approximately four in ten councils spent nothing on security training in 2020 (39.2%).

Of the councils that spent nothing, the majority stated they conduct in-house training at no expense. However, others reported that no training schemes were in place. Some councils offered optional training courses and others only mandated training for new employees.

One council declined to provide a training spend figure but disclosed that 0.01% of its annual Infortmation Communications and Technology (ICT) budget was allocated to security training. At the other end of the scale, one council spent £38,873 on training over the same period. This is the same council that reported 29 data breaches to the ICO in 2020.

Figure 5: *Security spend by council size – all UK councils*

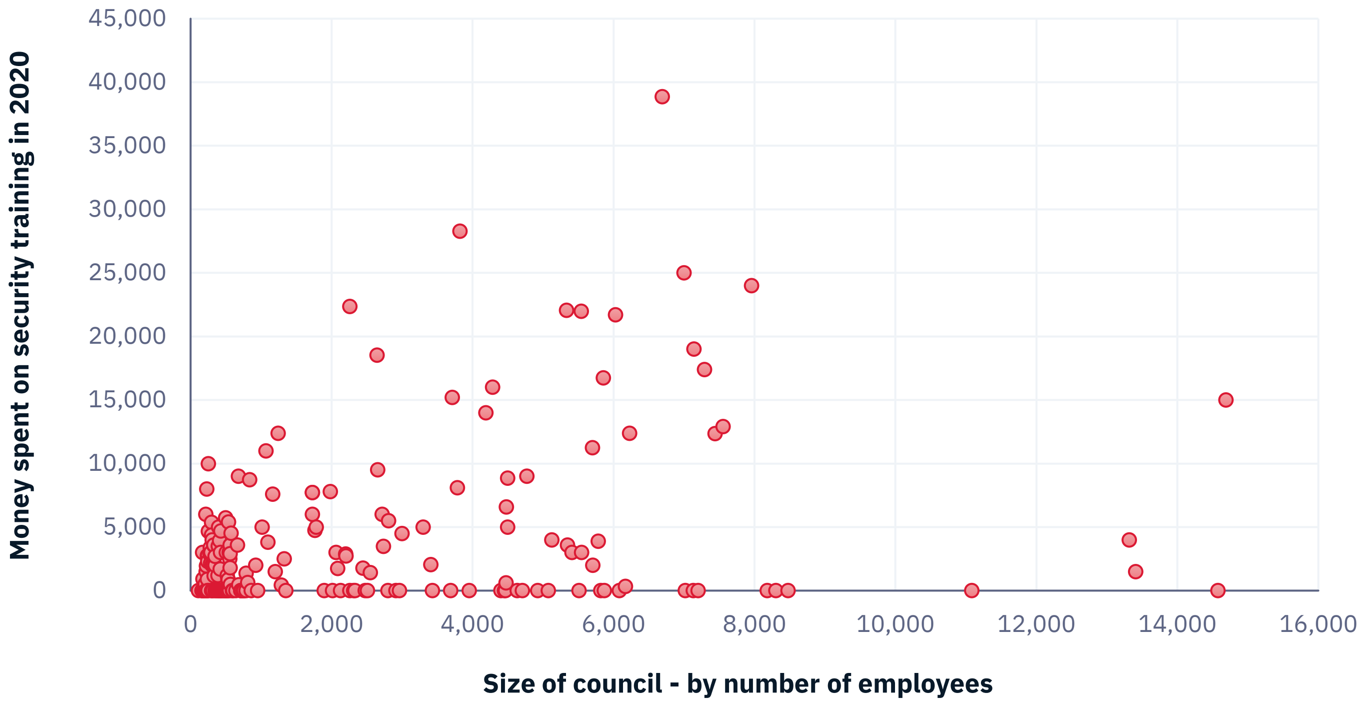
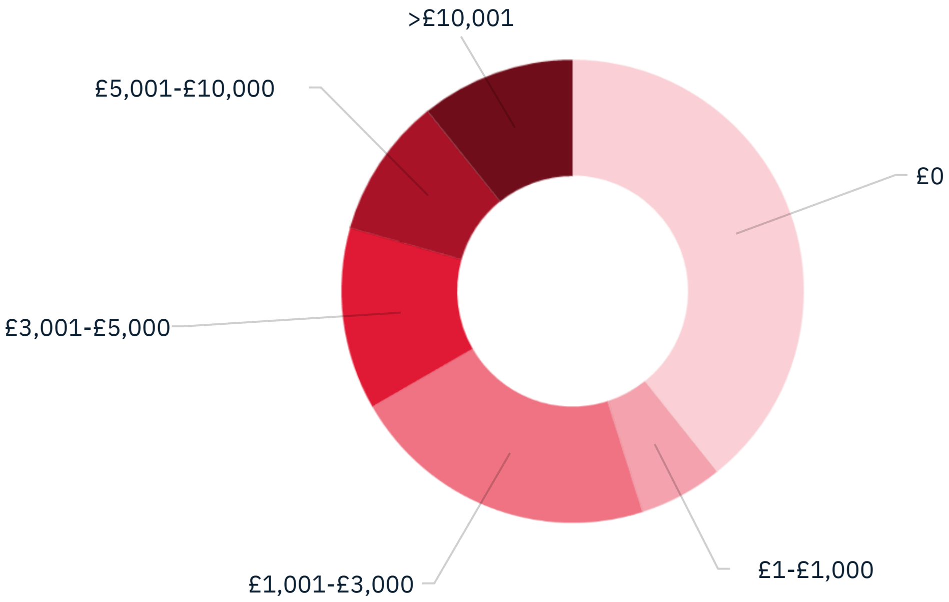


Figure 5 clearly demonstrates the disparities in security training spend across councils. Our analysis showed that county councils spend considerably more on cyber security training compared to other types of councils, averaging £8,995 per year. This is most likely as a result of their greater size and number of employees. However, although larger councils typically spend more, there are several outliers to this trend. For example, over a third of councils (36%) with more than 5,000 employees spent nothing on security training.

Figure 6: *Percentage breakdown of cyber security training spend by UK councils*

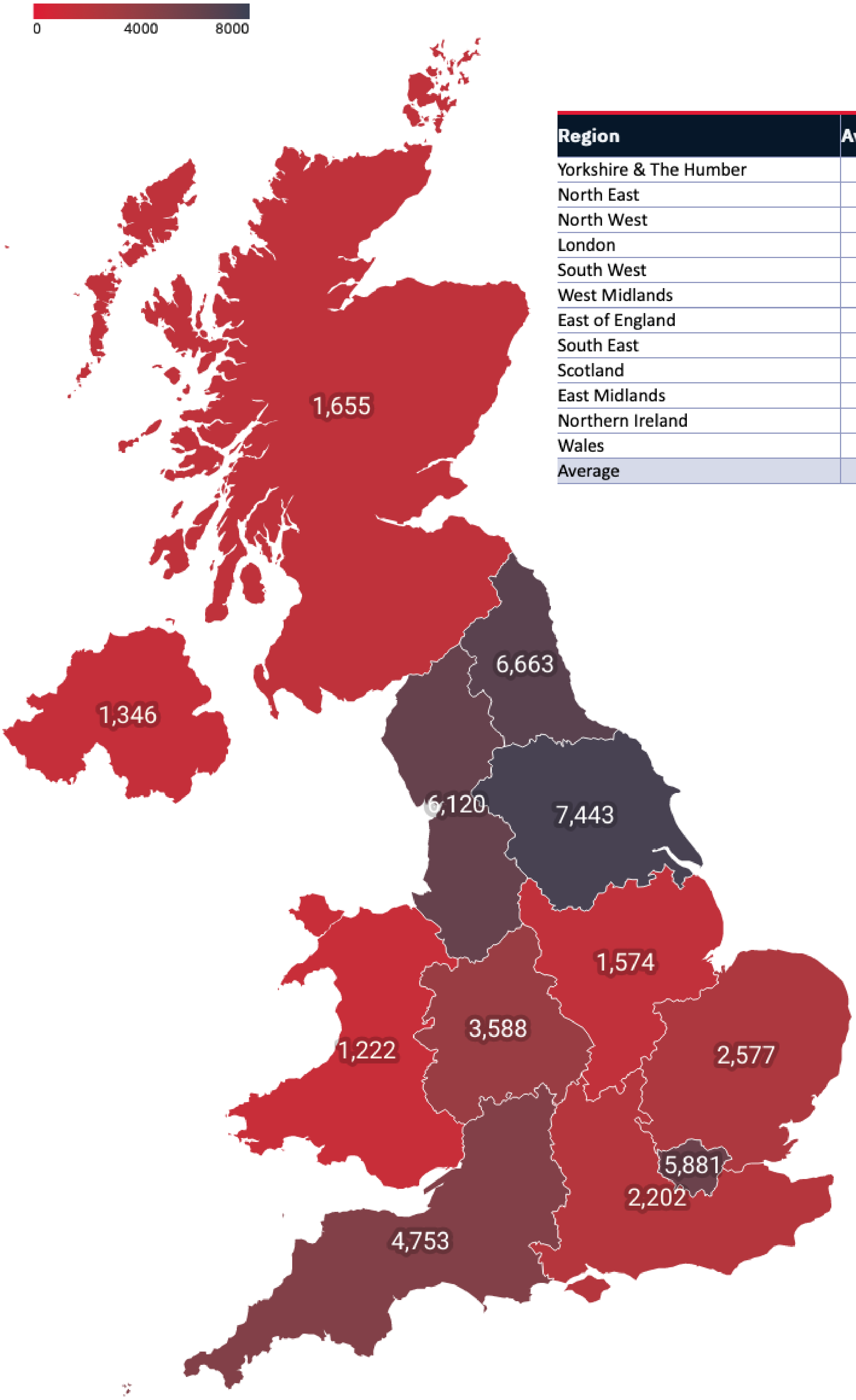


The average spend on cyber security training among city, district, borough and unitary councils in the UK in 2020 was £3,343.

Examining the average figure by country also reveals disparities. On average, councils in England spent £4,256 on cyber security training. The equivalent figures for Wales (£1,222), Northern Ireland (£1,346) and Scotland (£1,655) were significantly less.

Analysing security by region (see Figure 7 overleaf) reveals a slight north/south divide in England on training spend, with northern councils generally investing more. Yorkshire & The Humber has the highest average spend by council at £7,443. In London, the average spend is £5,881.

Figure 7: *Security training spend by all UK councils per region*



Region	Average 2020 spend
Yorkshire & The Humber	£7,443
North East	£6,663
North West	£6,120
London	£5,881
South West	£4,753
West Midlands	£3,588
East of England	£2,577
South East	£2,202
Scotland	£1,655
East Midlands	£1,574
Northern Ireland	£1,346
Wales	£1,222
Average	£3,343

What we say

“The fact that approximately half of council employees across the UK didn’t receive security training in 2020 is concerning. Annual security training sessions should be a minimum requirement for all staff, covering data protection, compliance and phishing awareness, among other areas.

“There are a lot of reasons why it makes sense for councils to set their own security budgets. However, far more consistency had been anticipated across different local authorities. The gap in security training spend across different councils is vast. Security training can be incredibly valuable. Cyber threats are always evolving so it’s important to keep skills up to date.”

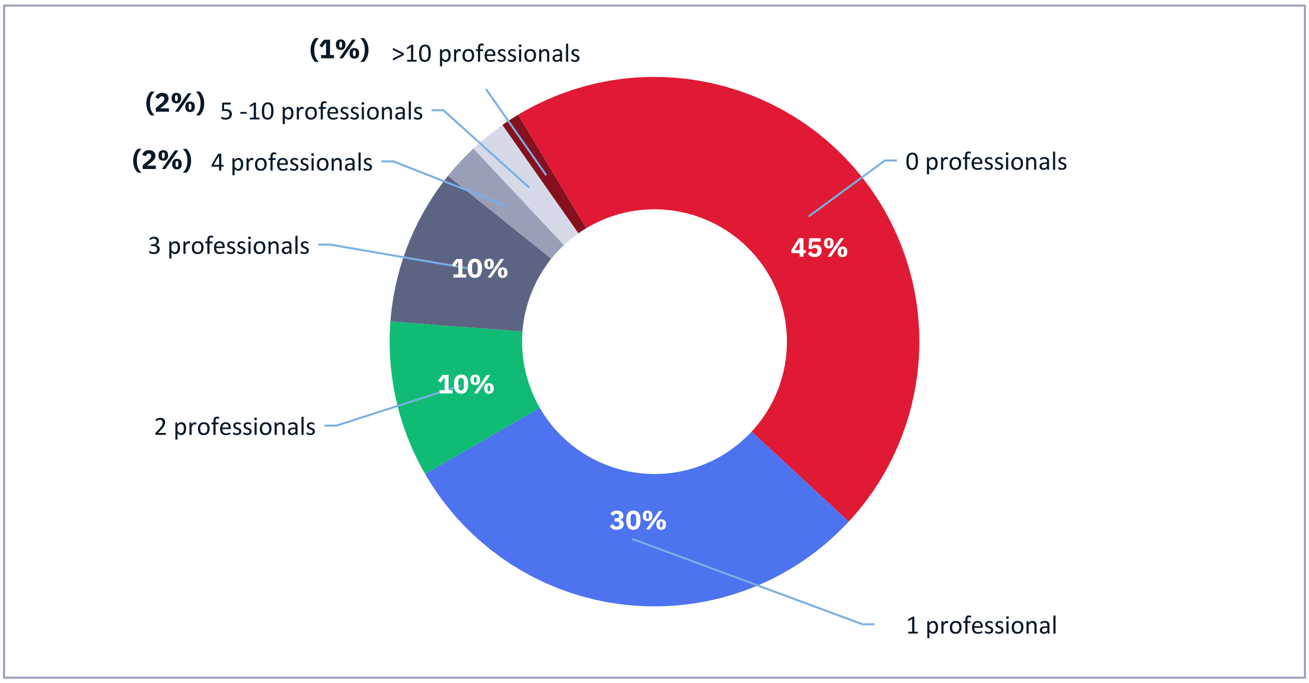
4. Security qualifications

4.1. A lack of qualified security professionals

Our research reveals that just over 45% of councils employ no staff with recognised security qualifications. Across the UK, councils employ, on average, one security professional per 2,141 employees, which is on a par with NHS trusts (as discovered in a previous Redscan FOI analysis).

Many councils responded that they outsource all their IT security functions, citing this as a reason they do not employ qualified professionals in house.

Figure 8: *Number of qualified security professionals employed by councils*



What we say

“It’s interesting to note that a significant number of councils identified outsourcing as a solution to their cyber security challenges. However, in addition to the benefits of accessing external support, as and when required, councils should have a strategy for ensuring key cyber security roles are staffed in-house with appropriately skilled individuals. Given the need to keep up with the latest threats, organisations need to ensure they have a strategy for upskilling existing staff.”

5. Report conclusion

When it comes to cyber security, there is no room for complacency. Every council has thousands of citizens depending on its services daily. Going offline due to a cyber-attack can deny people access to critical services.

To minimise the impact of data breaches, it is important that councils are constantly prepared to prevent, detect and respond to attacks. While our findings show that councils are taking some steps to achieve this, approaches vary widely and, in many cases, are not enough.

Our analysis shows that there is significant room for councils to improve their readiness to tackle both current risks as well as those which will emerge in the future.

Notes

Redscan submitted FOI requests to 398 borough, district, unitary and county councils on 8 January 2021 and received responses from 265 (63%) by 1 March 2021.

About Redscan, A Kroll Business

Redscan is an award-winning provider of managed security services, specialising in Managed Detection and Response, Penetration Testing and Red Teaming. As of March 2021, Redscan is now part of Kroll, the world's premier provider of services and digital products related to governance, risk and transparency.

Redscan works with organisations operating in a wide range of industry sectors. In the public sector, Redscan helps organisations to comply with the GDPR and NIS Regulations, as well as the Public Services Network Code of Connection (CoCo).

About Kroll

Kroll is the world's premier provider of services and digital products related to governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.

REDSCAN

A KROLL BUSINESS

☎ 0800 107 6098 ✉ info@redscan.com www.redscan.com