CHECK POINT™

PSE
PUBLIC SECTOR EXECUTIVE

CYBER SECURITY:

The heart and soul of trust between citizens and public sector organisations

AUTUMN 2023

Dan Benn,
Lead Journalist,
Public Sector Executive

Deryck Mitchelson,
Global CISO,
Check Point Software Technologies

Keith Joy,
Head of Digital & Technical Infrastructure,
University of the Arts London

DERYCK MITCHELSON:

EMEA Field CISO, Check Point

Deryck is a commercially focused C-suite executive, distinguished by expertise in cyber security and cloud, with global experience across both private and public sectors. His leadership in Consulting, Oil and Gas, and Healthcare provides Deryck with the platform for building and delivering IT and Security strategies and the application of emerging technologies, delivering a positive impact on both business goals and bottom line. In his current role at Check Point he acts as a security evangelist, advising C-Suite leaders on digital transformation, underpinned by security resilience and strategy. He is a recognized thought-leader and visionary, named in the top 20 IT influencers in the UK by Computer Weekly and winner of Holyrood's prestigious digital leader of the year award, amongst others.

KEITH JOY:

Head of Digital & Technical Infrastructure, University of the Arts London

Keith has spent the last three decades in senior leaderships roles responsible for technical adoption and digital transformation. He is recognised for uniting teams of diverse engineers, with highly technical specialisms, towards new ways of collaborative working which deliver against business objectives. Whilst maintaining a high level of technical acumen, Keith takes a lateral approach to aligning business processes with IT systems, earning him respect from both engineers and organisational partners alike. With a career which spans a range of public and private sector organisations - including local government, education, private enterprises and managed service providers - Keith has a unique perspective on the challenges facing organisation across the various aspects of services, systems and security.

INTRODUCTION

Public sector organisations play a crucial role in providing a wide range of services and support to citizens. They are responsible for delivering aspects of public welfare, governance, infrastructure, housing, healthcare and education to a population that is set to reach 72 million by 2041.

As the backbone of the economy, the services that sit within public sector are prime targets for cybercriminals. According to Check Point Research, the most impacted industry in the UK is Education/ Research, with an organisation facing 3,086 cyberattacks per week over the last six months. This is 56% more than the second most targeted sector, Government/Military.

It is no surprise that public-funded services are the hardest hit given the volume and sensitivity of the data they hold, and the far-reaching consequences that a cyberattack can have. They can carry heavy financial losses due to the costs of settling ransomware demands, mitigating the attack, recovering data, restoring systems, and implementing security measures to prevent future incidents. This could be detrimental given the limited budgets in the public sector. There may also be legal and regulatory fines for failing to adequately protect sensitive information, with the ICO issuing 34 fines in 2022 totalling £16m.

Cybersecurity incidents can also erode public trust in government institutions and services. If citizens feel that their personal data is not being adequately protected, they might be hesitant to interact with them, affecting overall engagement and participation. Finally, it may impact the long-term perception of the government's ability to protect citizens' data and provide secure services.

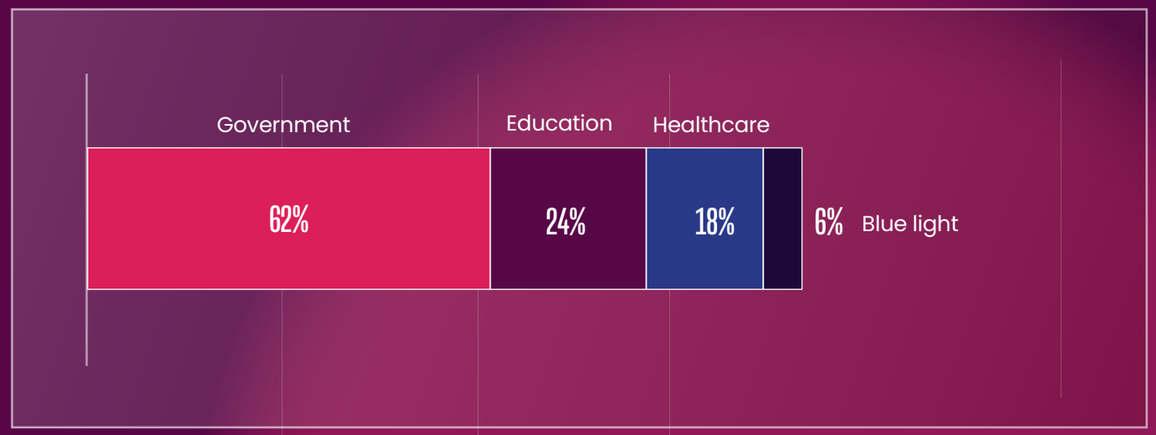
To mitigate these impacts, the UK public sector needs to invest in robust cybersecurity measures to build up their cyber resilience. This may include regular training for staff, incident response plans, and collaboration with cybersecurity experts. It also relies on public-private partnerships and international cooperation to combat increasingly sophisticated cyber threats.

UNDERSTANDING THE PUBLIC SECTOR CYBERSECURITY LANDSCAPE

To assess the perception and effectiveness of cybersecurity in the public sector, Check Point Software conducted a survey to look into why security decisions are made, the priorities that the sector focuses on, and how many vendors an organisation might employ to deliver their entire cyber posture.

Public Sector in 2023, saw 136 respondents across numerous areas of the public sector. 62% of respondents were from government, with 24% coming from education, 18% from healthcare, and 6% of the responses coming from people in blue light and justice organisations. Of these organisations, there was also a spread of different roles, with 56% of the respondents being in senior IT leadership role. The remaining 44% of respondents included positions such as Councillor, Compliance Officer, and Board Member.

After conducting the research, Public Sector Executive (PSE) spoke with Deryck Mitchelson (Global CISO), from Check Point Software, and Keith Joy (Head of Digital & Technical Infrastructure), from the University of the Arts London, about how vital cybersecurity is and how best to approach such a crucial issue.



Breakout of survey respondents based on sector

UNDERESTIMATION

The ideal place to start when looking at how best to approach cybersecurity is to look at how pressing many people believe their security issues are. The survey found that almost half (47%) of the respondents were confident that their cybersecurity system would find a breach, with 21% saying that they were very confident a breach would be detected. Just over 30% of the respondents, however, were somehow confident or not confident at all. These levels of confidence were matched when respondents were asked about their confidence in whether security systems would be able to discover whether or not any data had been stolen. 47% and 17% of the respondents were either confident or very confident in their cybersecurity system's ability.

Whilst the entire sector might understand the importance of the information that they hold, there may be an element of overconfidence when it comes to just how protected they are. This is something that was referred to by Keith Joy, CTO at University of the Arts London, who said:

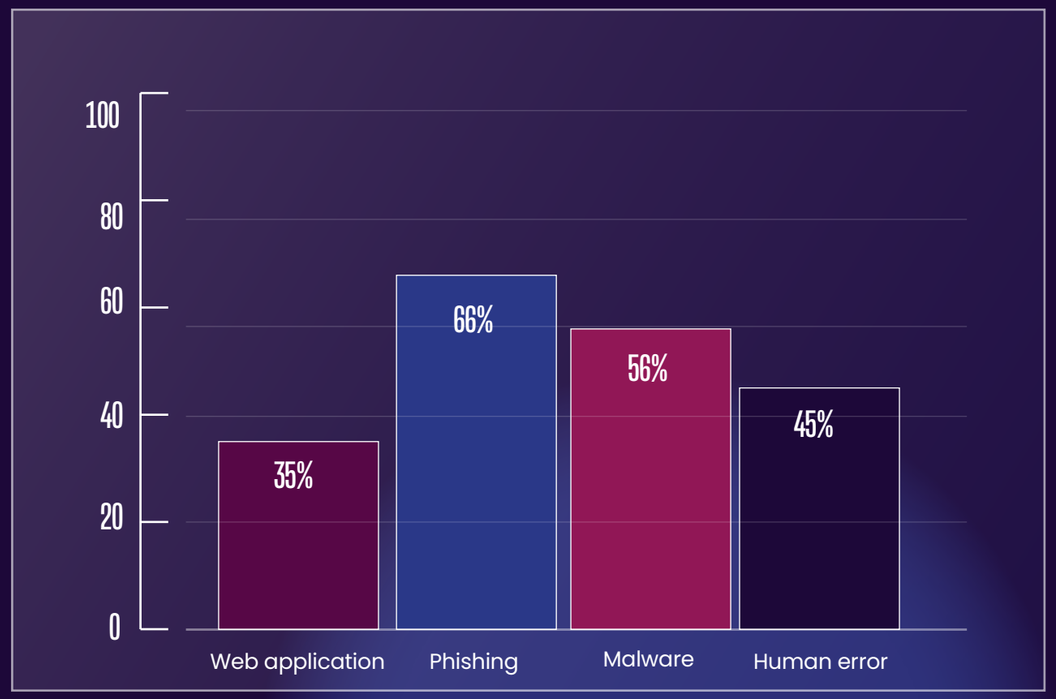
"often people think that they're fine and they're protected until something goes wrong." Keith developed this point, talking about how the sector might anticipate the risk of a cyberattack. He added: "I think people do underestimate the potential avenues through which they can suffer a cyberattack or data breach."

"We often think about big ticket items when we ask these sorts of questions, but there are so many smaller avenues of entry into an organisation. There are so many things like Bitcoin mining, for example, that don't necessarily require elevated permissions to install, and, in themselves, they are not necessarily classed as viruses because they're legitimate applications. But if you get a classroom of high-performance computers with large graphics cards in them, they'd be a great pick for someone who wants to do a bit of mining and can set something up overnight."

"Those sorts of areas aren't necessarily going to set off alarm bells and say, 'there's a security breach' and your antivirus might not even pick it up, but it is still unwanted software running on computers."

The public sector is one of the most targeted sectors when it comes to cybersecurity breaches, with the Government Cyber Security Strategy stating that approximately 40% of the 777 cybersecurity incidents that were managed by the National Cyber Security Centre (NCSC) between September 2020 and August 2021 affected the public sector.

The survey also found a general lack of awareness across the public sector about the entry points and lateral spread of cyberattacks. When asked "which types of cyberattacks pose a higher risk for your organisation" only 47 of the 136 respondents (35%) selected web application attack as high-risk. This was the third least selected option, with phishing (66%) and malware (56%) being the two most popular responses. Notably, the third most common answer was human error, which was selected by 45% of the respondents. Whilst this indicates a lack of confidence in people inside an organisation, this conflicted with the results of another question in the survey. The question suggested that 99% of cybersecurity breaches by 2025 would be through human error and, with this in mind, asked how confident the survey's participants are that workloads and data are being monitored and secured adequately. In response to this question, 43% of the participants stated that they are confident of adequate monitoring and security, with 33% and 14% being somehow confident and very confident respectively. Only 7% of the respondents were not confident at all.



Which types of cyberattacks pose a higher risk to your organization

This is an interesting development given the Department for Science, Innovation and Technology's Cyber security skills in the UK labour market 2023 report stated that 50% of all businesses in the UK have a basic cyber security skills gap, while 33% have an advanced gap in cyber security skills. These figures are similar to those in 2022 and 2021, showing that despite the ongoing digital transformation developments, skills aren't developing at the same rate. Alongside those particular figures, the report also identified a 30% increase of cybersecurity job postings in comparison to the previous year, with the number increasing to 160,035.

One reason for a hesitance to blame the workforce could be the recent uptake in remote working, with many people no longer office-based full time since the Covid-19 pandemic forced offices around the world to shut. When asked about whether or not they would agree that having a large number of remote workers increases the risks of cybersecurity being compromised when compared to traditional office-based working, 62% of the respondents either agreed or strongly agreed, with 21% either disagreed or strongly disagreeing.

Deryck Mitchelson, CISO at Check Point, and Keith noted why there could be a slight discrepancy between the answers to the different questions. Keith said: "The wording of the first question leads responders to think about technical solutions, whilst the second question steers towards users. It shows more trust in technology than in the people we employ to use it. Organisations may think that they've put lots of things in place technically, but a lack of people training and robust processes can easily trip this up."

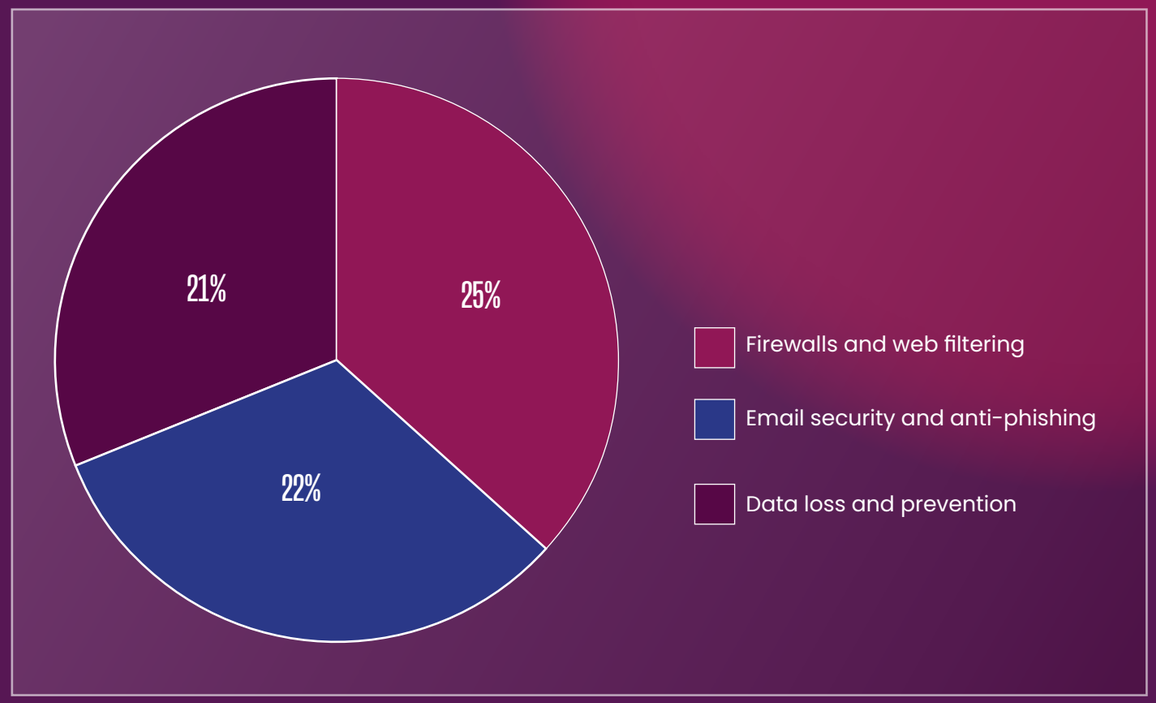
Deryck expanded this point by saying that "you would always try and build a programme around guardrails that are around the people and processes. You do need to educate your people as they're the first line of defence, but you also want to make sure that you build a really strong second line of defence behind them."

SECURITY SPENDING

When considering other challenges that might be faced by public sector organisations when they are trying to improve their cybersecurity, another one that will likely keep cropping up is spending. A lot has been made of the issues that are ongoing with public sector finances, and that was reflected in the results of the Check Point survey. When asked what the biggest obstacle to achieving the desired cybersecurity posture was, the most common response was budget constraints, with 57% of the selections. Keith gave his view on this saying: “I think you always believe that you can do more with a bigger budget. That’s the same with everything and when we focus, particularly around security, there is so much that we would like to do and a lot of it comes down to buying, essentially, expensive products and tools to do that. Of course, we can never expect a blank cheque, so evaluating and understanding areas of vulnerability then prioritising around risk is key when determining where to spend.”

Deryck added his own spin onto the argument of the importance of budget restrictions, saying that it isn’t necessarily the budget itself that poses a challenge, but the way that it comes. Deryck said: “Your budget would come on a year-by-year basis, but it wouldn’t always get to you right at the start of the financial year, there would be settlements and budget agreements. By the time the budgets actually come down from those who are providing the central budget and you’ve studied it to see how much you’re getting, you had to try and change your strategy in order to actually implement it. Concerns I always had was timing that often didn’t align against what I was trying to deliver.”

It is also worth considering where budgets are actually being spent across the sector. Through the survey, respondents in a number of roles across the public sector were asked which specific area they are investing in the most to improve their cybersecurity. The most selected option, with 25% of the vote, was firewalls and web filtering, the second most chosen option was email security and anti-phishing with 22%, and the third, with 21%, was data loss and prevention.



Priority of cyber security spend for public sector

THE CHECK POINT APPROACH

Check Point's approach to cybersecurity seems to be a natural solution to all of the issues raised above, thanks to the preventative strategy that they employ. With the number of concerns that are raised through the survey regarding confidence in breaches being picked up, a preventative strategy has the ability to solve many organisational problems. Deryck touched on this, saying: "Check Point's belief is that you need to have the same level of preventative security and threat intelligence that runs across every single aspect of your digital estate.

"If there are any blind spots or points of weakness, then the threat actor will take advantage of it, but this is very much what Check Point's ethos is around. If you look at security as a holistic problem, rather than as a single problem that fixes a network, perimeter, or cloud, then you get a much higher level of end-to-end protection. That means that the chances are, you'll be able to prevent something."

The importance of Deryck's point about using a preventative strategy is highlighted above, however, with prevention being the third most invested in area of security, many organisations across the sector are either not thinking about prevention, or simply aren't aware of the benefits that it can bring.

Keith added another angle on the topic of preventative security, linking back to the arguments that were raised above regarding complacency.

"WE SHOULD ALL BE AIMING FOR PREVENTION, 100%, BUT WE SHOULD ALSO ACCEPT AND UNDERSTAND THAT PREVENTION IS NOT AN INFALLIBLE DESTINATION, IT'S A CONSTANTLY MOVING TARGET WHICH WE MUST STRIVE TOWARDS IN ORDER TO STAY AHEAD OF MALICIOUS ACTORS."

He said: "Prevention is always better than cure, however the worry is that if we talk too much about prevention then people could become complacent.

"We can build tools that help us prevent attack vectors, but we know that as soon as you do then someone will find another way around. It's very hard to stay one step ahead of the imagination of the people that are determined to get through your security systems.

"We should all be aiming for prevention, 100%, but we should also accept and understand that prevention is

not an infallible destination, it's a constantly moving target which we must strive towards in order to stay ahead of malicious actors."

A further benefit of using Check Point's preventative method, is that organisations can reduce the number of security vendors that they require to keep their data and workflows secure. According to the survey, 67% of respondents stated that they have between one and nine security vendors. Of the remaining 33%, 15% said that they use between 10 and 19, 12% said that they use between 20 and 29 different vendors. Rather concerningly, 7% of the survey's participants stated that they use thirty or more vendors, something that is completely in contrast to the way that Check Point operate.

Bringing in a number of different vendors has its issues, something that was also mentioned in the survey. According to the participants, the biggest concern when it comes to the utilisation of multiple vendors is the fact that multiple different solutions require multiple skillsets, as 53% of the respondents stated that this was an issue.

Second to this concern – with 45% of responses - was the fact that, whilst there may be some overlaps in security coverage, organisations also run the risk of leaving some gaps. The third most chosen concern relating to this question, with 40% of the respondents selecting it, was the fact that additional complexity and an increased number of vendors has the potential to increase costs.

Considering the part that budgets and costs play, alongside upskilling the workforce, it would seem that a vendor that can provide end-to-end coverage would be the best option for an organisation in the public sector.

ABOUT CHECK POINT SOFTWARE TECHNOLOGIES LTD.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cybersecurity solutions to corporate enterprises and governments globally. Check Point Infinity's portfolio of solutions protects enterprises and public organizations from 5th generation cyberattacks with an industry leading catch rate of malware, ransomware, and other threats. Infinity comprises four core pillars delivering uncompromised security and generation V threat prevention across enterprise environments: Check Point Harmony, for remote users; Check Point CloudGuard, to automatically secure clouds; and Check Point Quantum, to protect network perimeters and datacenters, all controlled by the industry's most comprehensive, intuitive unified security management; Check Point Horizon, a prevention-first security operations suite. Check Point protects over 100,000 organizations of all sizes.

ABOUT UNIVERSITY OF THE ARTS LONDON.

University of the Arts London offers an extensive range of courses in art, design, fashion, communication and performing arts. UAL is ranked second in the world for Art and Design in the 2022 QS World University Rankings®.

The University is made up of 6 renowned Colleges: Camberwell College of Arts, Central Saint Martins, Chelsea College of Arts, London College of Communication, London College of Fashion and Wimbledon College of Arts.