computing research

RESEARCH PAPER

Endpoint security versus productivity in utilities: a false choice?

why the utilities sector does not have to choose between the securing of endpoints and the productivity of users – and security teams.

December 2020

Sponsored by BlackBerry Intelligent Security. Everywhere.

CONTENTS

Introduction

For some time now, the prevailing wisdom in technology circles is that strong cybersecurity and the productivity of workers – particularly remote workers – are fundamentally at odds. Workers, we are told, demand instant access to a full set of resources from any device without having to remember bothersome passwords, conducting multiple authentications, or having to navigate any other process of determining permissions. Often these needs are perceived as conflicting with cybersecurity objectives. If you make it difficult for workers to access the resources and platforms they need to get the job done, they will simply use insecure workarounds.

The tension between security best practises and the workforce's genuine desire to get the job done adds weight to the widely held perception that breaches are inevitable and that time and resources should subsequently be focused on remediation rather than on prevention.

Computing does not seek to challenge the view that breaches are inevitable. This is a universal truth – demonstrably a fact. *Computing*'s interviews with CIOs and CISOs consistently support this view, and it is a consistent finding in both our research and the recent history of utilities in the UK.

Nonetheless, despite the likelihood of breaches, it is possible to argue, and cogent to do so, that the wholesale elevation of remediation over prevention can result in the neglect of easily preventable breaches. Precious time and resource are expended remediating breaches that needn't occur, and as a consequence, security teams are on the back foot. This is not ideal when the frontline – the endpoint – is under assault like never before.

The organisations that pipe water, energy, and data into our homes are an enticing target for attackers. The critical importance of these organisations to infrastructure makes them high value for those intent on financial extortion or simply causing chaos. They also hold sensitive information about millions of customers, including financial and contact data. Utility companies are often targeted because they can be used so effectively as phishing lures. Possibly the best-known example of this could be seen in the huge Talk Talk data breach of several years ago. While the initial attack and its handling were a PR disaster, the stolen data was sold, and Talk Talk customers were targeted by criminals calling them and posing as Talk Talk engineers helping them to fix problems with their broad band – after they'd transferred payment of course.[1]

Utilities organisations tend to be large and widely distributed with a high incidence of remote and mobile working – even pre-pandemic – and the gradual transition to a lower carbon economy has meant that utilities have been leaders in digitisation. The utilities industry has also been disrupted by smaller start-ups, offering consumers greener services and competitive pricing, and larger established utilities providers have been driven to transform their legacy infrastructures into flexible, data driven, and predictive ecosystems. These systems focus on smart grid management, smart metering, and customer service – a trend which is only going to accelerate in pace following recent announcements on what is being billed as a green industrial revolution.[2]

[1] https://www.which.co.uk/news/2018/08/internet-router-hack-scam-targets-uk-homes/

[2] https://www.energylivenews.com/2020/11/18/boris-johnson-unveils-ten-point-plan-to-tackle-climate-change-deliver-net-zero-and-launch-a-green-industrial-revolution/

The highly connected – and fast-growing – nature of utilities infrastructure is at once a crown jewel and an Achilles heel. We all benefit from a greater eye on consumption and smart metering is a way to achieve that. Utilities companies are busy implementing strategies to derive insight from and monetise the data that all these devices provide. But their attack surface is growing steadily – and the interconnected reality of utility provision means that if an attack on one endpoint lands, all are vulnerable.

Many security problems have been aggravated by the pandemic – particularly those associated with remote working. Employees accessing grid networks from home carries a degree of risk that is far higher than when access is controlled within a corporate network, and at the same time, the demand for utilities became volatile. Fuel and energy consumption reduced as we all moved around less, and this reduction brought some technical challenges for energy providers. Other utilities saw demand skyrocket. The demand for Internet bandwidth and mobile data in particular went through the roof, as in many households during the week, multiple video calls, online schooling, and Joe Wicks PE lessons were often being conducted all at the same time.

The results shown in this research paper are drawn from a survey covering 100 IT professionals with responsibility for security strategy or implementation in utilities organisations.

Key findings include:

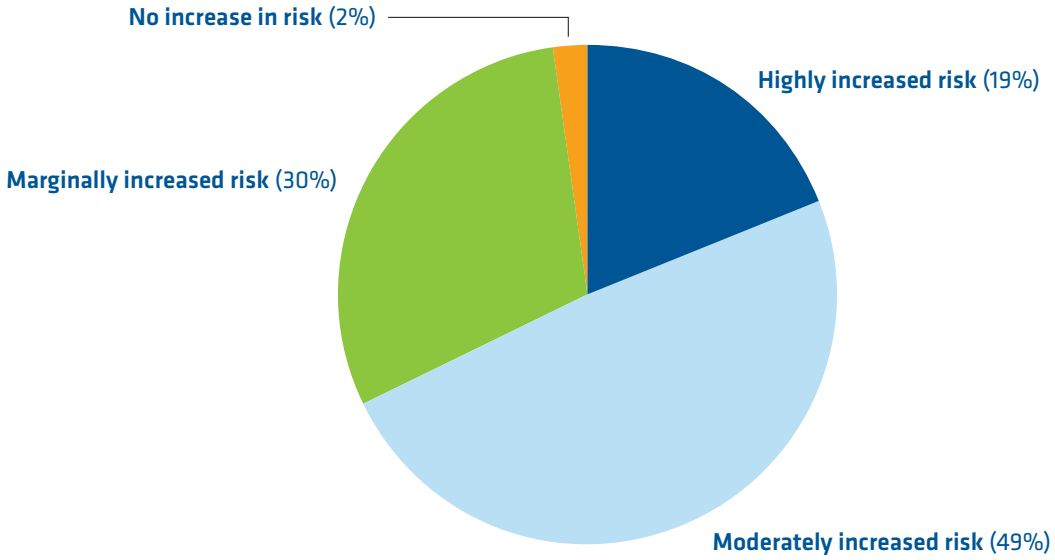
- There is considerably less confidence in remote endpoint security than security overall. 81% of contributors were either moderately or highly confident in overall security, but the proportion declaring themselves so for remote workers falls to 69%.
- IoT and Edge devices had already been subjected to attacks for 18% of those contributing from utility providers and there was a broad consensus that the increasing prevalence of such devices was increasing the security burden.
- 44% had experienced an increase in cybersecurity incidents as a result of pandemic-induced remote working.
- 53% of utilities firms in the survey reported that their remote infrastructure specifically had been targeted.
- 98% of contributors agree that the increase in remote working has increased risks to their cybersecurity.
- The top three most frequently experienced attacks experienced this year by utilities companies were phishing/spear phishing (71%) and then malware/ransomware (65%), followed by denial of service (29%).
- In excess of two-thirds agreed that their organisation's cybersecurity strategy had moved more towards a detect and remediate approach rather than prevention in recent years.
- In the event of a security incident, 28% of contributors had to investigate upwards of seven sources of data, and 15% had to investigate in excess of 10 sources.

Remote workers: the new frontline of cybersecurity

When making assertions about prevailing wisdoms – in this case the tension between security and productivity objectives – it's useful to check whether they are indeed still prevailing. *Computing* asked those contributing to our research from utilities organisations the extent to which they agreed that, *"at times in our organisation, the objectives of cybersecurity and productivity for remote and mobile workers clash"*. 66% agreed either somewhat or strongly. For the most part, tension between these objectives still exists.

The nature of the utilities sector means that it already had levels of remote working probably a little above the U.K. average prior to the pandemic. It's an industry which employs many field engineers and has a high percentage of key workers. However, 94% of contributors reported that the proportion of remote workers in their organisation had increased since March 2020.

Fig. 1 : What level of extra risk do you think these remote workers and their devices may pose for your cybersecurity?



Is this increase in remote working going to be sustained? While most will welcome recent news about the development of vaccines that can hopefully bring the pandemic to end, the scale of remote working that began in the Spring and is still ongoing means that office life is unlikely to return in its previous form. The degree to which we all go back to office-based working life is still a moot point but plunging commercial property values and the amount of vacant industrial units offer a hint as to what lies ahead. While many workers in utilities are field-based, 2020 has changed the face of the customer service and call centre work which is so important to utilities. Technology to enable this type of work to be conducted from home has been around for a while. What businesses lacked was the will to move away from more traditional models. A global pandemic concentrated minds, and remote working is likely to remain a key plank of critical infrastructure service delivery.

The problem is that all but 2% of our contributors believe that these employees and their devices are posing extra risks to cybersecurity. Some of the reasons for this increase in risks are not specific to utilities. On-site discussions have been replaced by video conferencing, the security of which has been the subject of much industry discussion since March. The use of collaboration and file sharing applications more suited to consumers is problematic if confidential data, particularly that pertaining to customers, is being shared via such mediums.

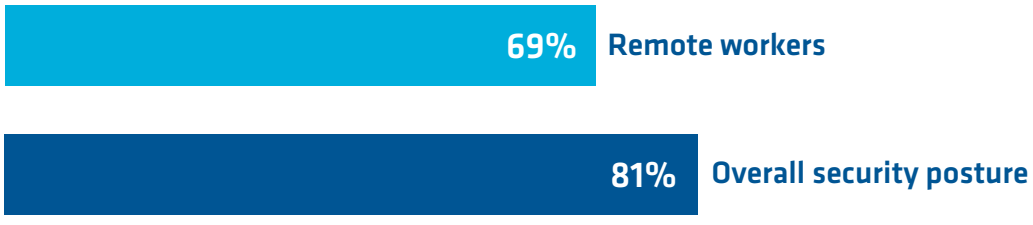
Other universal problems include the temptation for employees to work on newer, personally owned laptops and tablets instead of relying on their organisation's standard-issue kit, which is rarely at the cutting edge of technology. Personally owned devices are often shared with children and partners who may visit sites which are normally avoided on corporate endpoints. The combination of this greater variation in usage patterns, consumer grade defences on these laptops, and the distractions which invariably arise in a domestic environment presents a significantly increased attack surface for attackers to exploit.

Quiet working spaces are also hotly contested in many family homes, and those living in shared accommodation face bigger challenges. Amid this distraction, the likelihood of unwittingly clicking on a clever – or even not so clever – phishing email has increased, and the nature and likely extent of Shadow IT means that once those clicks have happened, defences are easily bypassed. Attackers are on the hunt for privileged accounts – those with elevated user rights – where sensitive data and applications can be accessed without all the trouble and bother of penetrating expensive defences like firewalls.

Escalating risks and IoT

The increased risks that the forced home working revolution has posed would be less of an issue if cybersecurity professionals had as much confidence in the security tools covering mobile devices and remote workers as they did in cybersecurity overall. Unfortunately, they don't. 81% were either moderately or highly confident in overall security but the proportion expressing the same level of confidence drops to 69% for remote workers. Equally, the proportion declaring themselves not particularly confident increases from 3% to 8%.

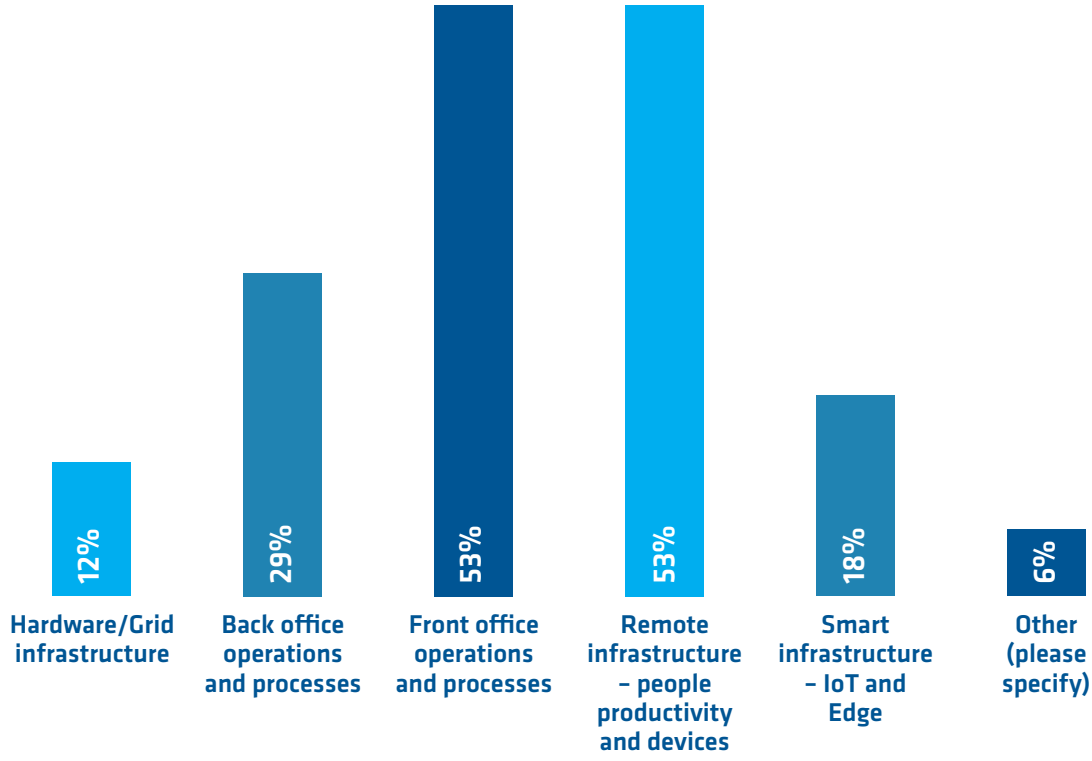
Fig. 2 : Confidence in overall security posture vs. confidence in security of remote workers – moderately or highly confident



The fact that more than two-thirds of contributors still had such a level of confidence in their endpoint security is an interesting finding when viewed in light of another – that 44% of contributors said their organisation had experienced an increase in cybersecurity incidents as a result of pandemic-induced remote working. This compares unfavourably with a rate of 32% for the public sector who are probably the most similar vertical sector in terms of the importance of services provided. These figures suggest that utilities are being targeted and that some of the confidence in endpoint security is misplaced.

Further weight is added to this line of argument by the findings illustrated below. 53% of utilities-based contributors reported that their remote infrastructure had been targeted.

Fig. 3 : Thinking of recent attacks – successful or not – which parts of your infrastructure have been targeted? Please choose all that apply



In addition to remote infrastructure, the challenge faced by the utilities industry, perhaps more than any other, is the scale of IoT and also Edge computing within their operational technology (OT) estates – all those smart meters and grid sensors feeding back usage data. Not only is the scale of the attack surface vast – much of it is in the hands of consumers themselves. Placing the onus on consumers to manage the security of their devices is unlikely to end well. Cybersecurity professionals have long understood the reluctance of users to implement upgrades and patches themselves, and indeed their relaxed attitudes towards the concept of cybersecurity generally – and it's not just their own products that cause a risk. Some recent tests on smart doorbells from the

usual digital marketplaces found that 11 had significant security vulnerabilities, some of which left customers having their wireless credentials sent unencrypted across public networks.[3] This renders any other connected smart device vulnerable.

18% of survey contributors reported their Smart IoT and Edge infrastructure had already been subjected to attacks. *Computing* also asked more broadly what impact IoT and Edge devices had on estate management. A selection of responses are as follows:

"Not so much IoT within a corporate environment, but operational technology (OT) footprint growth has outpaced corporate IT. Increased convergence makes alignment key."

"Greater need for endpoint security."

"Increased the cybersecurity risk, meaning that more has had to be spent to ensure security."

"Harder to manage short term as more data points, but better long term as more proactive."

"Significant. Is driving a move from analogue to digital sensor/control networks."

As the diagram in figure three illustrates, the risks facing critical infrastructure providers are not theoretical. A string of attacks on Ukrainian energy providers a few years ago showed that hostile states could and would cause blackouts as well as target a number of other critical services such as railways.[4] In the U.K., it has been clear that the energy and telecommunications sectors have been targeted for the last few years. In 2017, this was openly acknowledged by the U.K. government.[5]

Adding insult to near injury, cyber criminals were not slow to exploit the pandemic, and they are not sentimental about the human cost of their activities.

Attacks and remediation

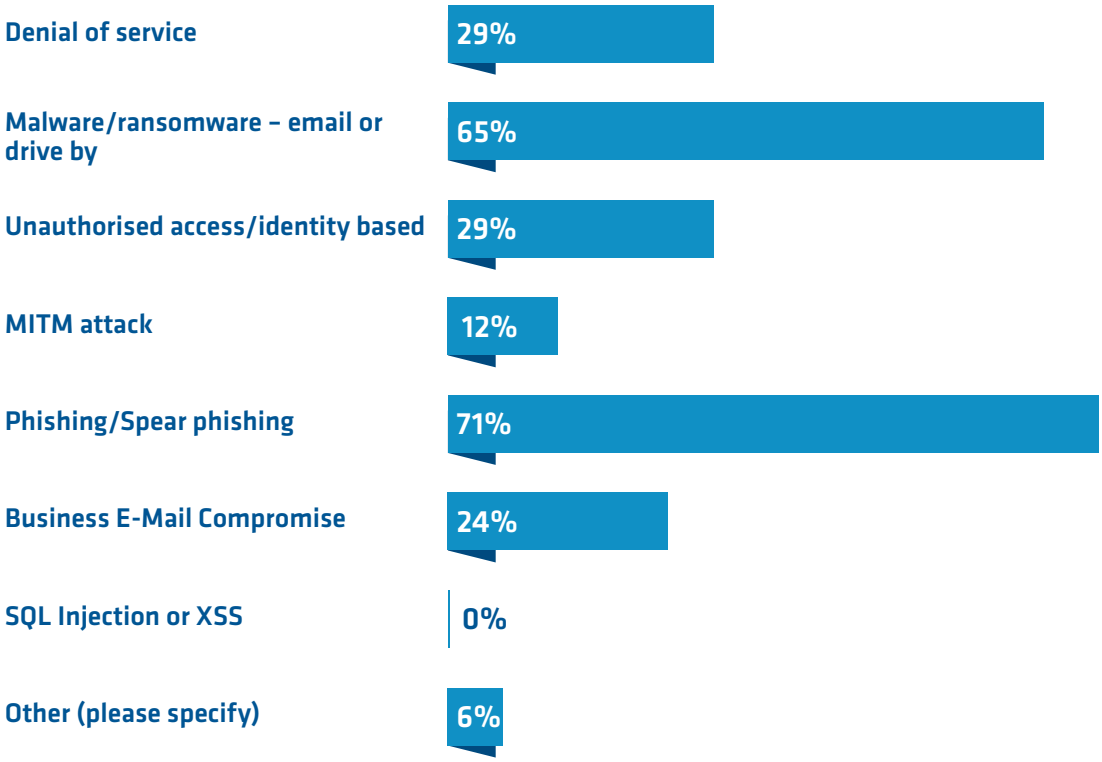
The top three most frequent attacks experienced by contributors from the utilities sector were phishing/spear phishing, closely followed by malware/ransomware, and then denial of service attacks.

[3] https://www.which.co.uk/news/2020/11/the-smart-video-doorbells-letting-hackers-into-your-home/

[4] https://www.bbc.co.uk/news/technology-38573074

[5] https://news.sky.com/story/russian-hackers-targeting-uk-energy-and-telecoms-sector-11127641

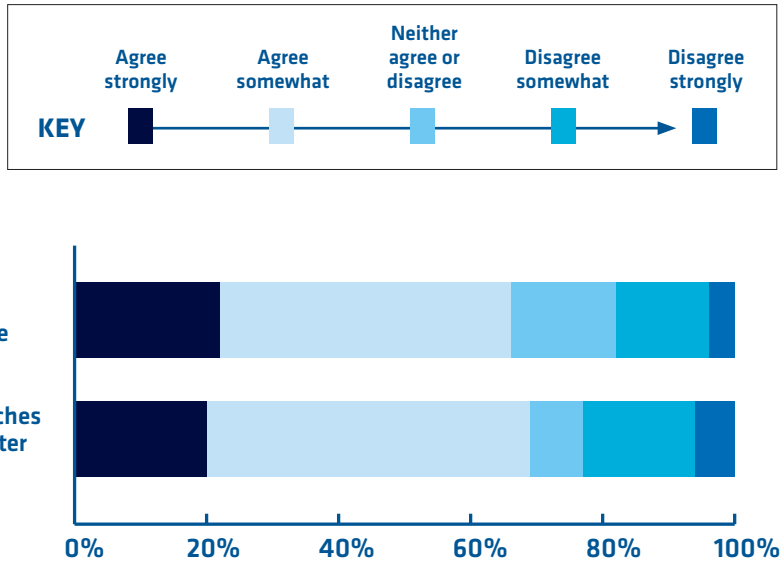
Fig. 4 : What kind of attacks have you experienced this year?
Please select all that apply



They are closely related threats. Attackers often target specific users with phishing attacks, having identified who they are, and what access rights they will likely have, in advance. This can be SysAdmins with elevated rights to access the network and devices and applications on it. It could be technicians with access to SCADA systems or it could be individuals employed in customer service or finance with the authority and access to make payments. Whatever the approach – from phishing to credential theft – the target is usually privileged accounts. It is far easier to gain access to systems and data via privileged accounts than to attempt to circumnavigate defences like firewalls. This makes remote workers the attack vector of choice for criminals – and the huge increase in numbers of remote workers at utility companies has increased the size of the attack surface really rather significantly.

A degree of fatalism is perhaps understandable in the minds of utilities security teams. 69% agreed to at least some extent that, *"we have accepted that some breaches of cybersecurity will occur no matter how good our defences are".* Certainly, given the critical nature of the infrastructure, having security incident response plans and some sort of automated remediation strategy is a must have. Furthermore, figure five suggests a clear shift to a detect and remediate rather than a preventative approach to cybersecurity.

Fig. 5 : To what extent would you say that your organisation's cyber security strategy has moved more towards a detect and remediate approach rather than prevention in recent years?

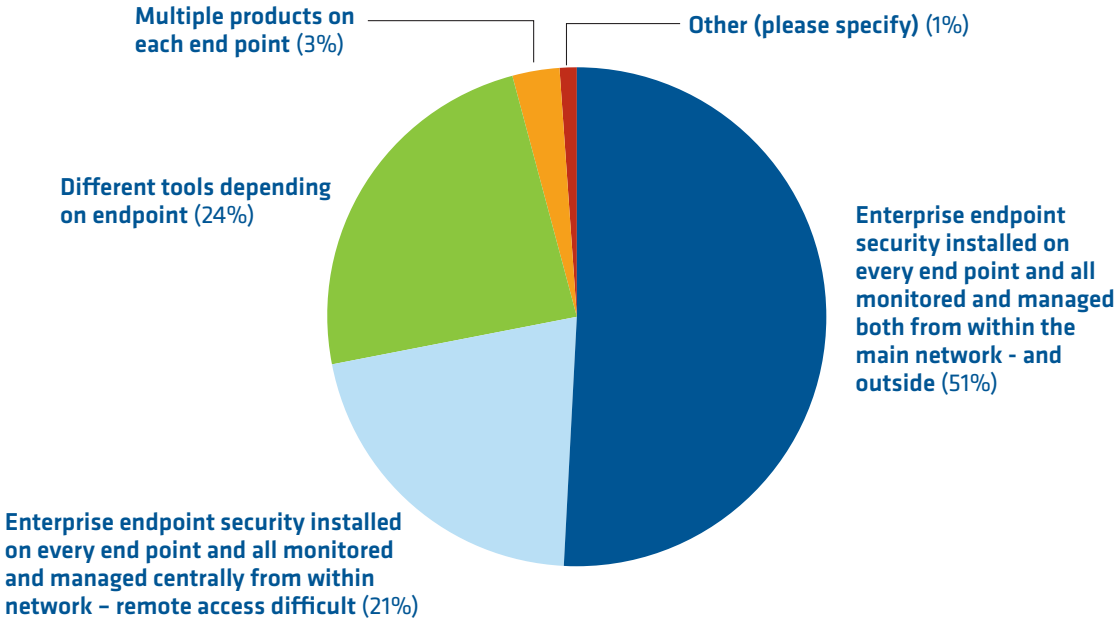


This isn't a particularly surprising finding. Nor is it limited to organisations in the utilities sector.

It is also a commonplace in *Computing* research to find that cybersecurity teams are understaffed and overworked, struggling with the sheer volume of incidents requiring investigation, often working with a series of different technologies that have been installed piecemeal over time as new threats emerged, and struggling to put together a picture of what *may* have happened from a variety of different sources – some on-premises, some in the cloud.

How are utilities organisations protecting their endpoints within their operational technology estates? The picture is highly varied. While 51% have endpoint security all manageable from inside and outside the relevant network, 22% are struggling with remote access for endpoint security, which is profoundly unhelpful in our present environment. 24% had more than one endpoint security product to manage, depending on the endpoints, and 3% had multiple products on each endpoint.

Fig. 6 : How are you managing endpoint security specifically within your operational technology estate?

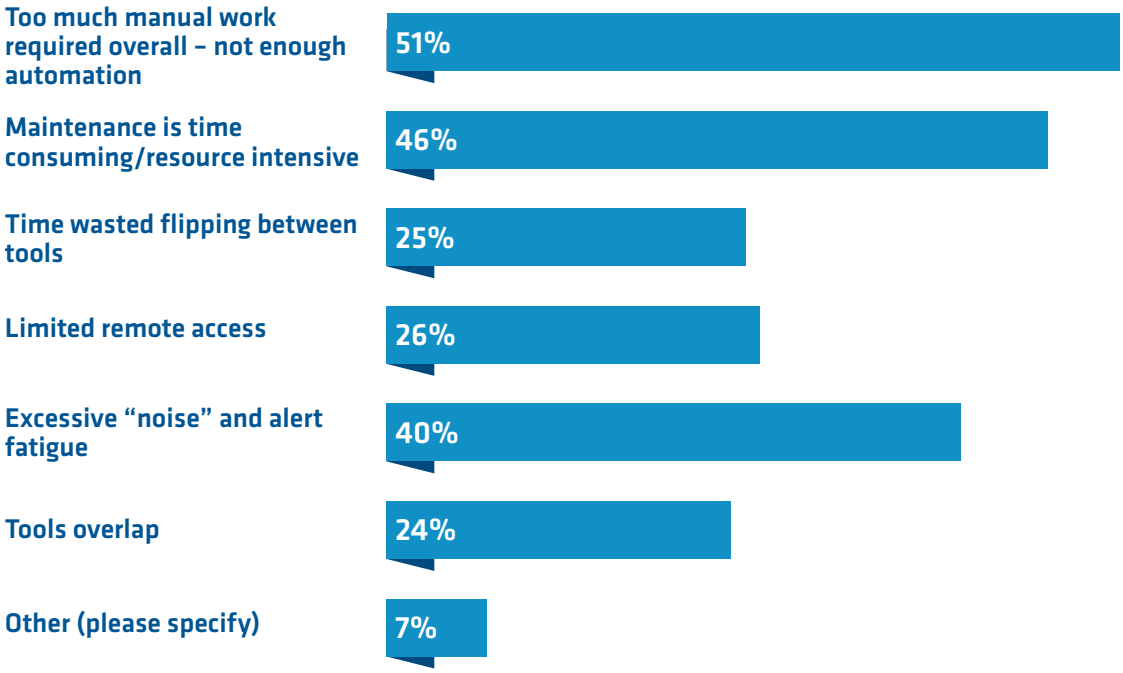


The proportion of contributors struggling with multiple products gives us a clue as to the extent of some of the challenges security teams in utilities organisations face – and indeed in many other enterprises. Too much work in cybersecurity is done via manual processes, maintenance is both time consuming and resource intensive, there is excessive noise generating alert fatigue, and remote access is limit.

Computing's research also shone light on a specific aspect of this issue – that of the amount of data sources cybersecurity teams have to work with to remediate a problem. In the event of an incident, 44% of contributors have to interrogate four to six sources of data. 28% of contributors had to investigate upwards of seven sources of data. 15% overall had to deal with *more than 10 sources*.

Another challenge facing large utility providers in particular is visibility of their vast and growing estates. When asked to indicate their confidence in the visibility of their mobile device estates, only 35% of contributors expressed a high level of confidence. Any reader of this paper is highly likely to be familiar with the concept that it is impossible to secure what you can't see.

Fig. 7 : Please indicate if you are experiencing any of the following challenges with your cybersecurity incident detection and remediation.
Please select all that apply



There are serious implications arising from both tool sprawl and compromised visibility. Cybersecurity remediation in these circumstances is complex, painstaking, and time-consuming work – and with so many false flags, is also potentially demoralising. The more tools that staff have to use, the tougher the task gets, and the pandemic has exacerbated an already difficult situation. Separate research by *Computing*[6] has shown that IT professionals across the board are more likely to be at home than their peers, and that their managers are finding it more challenging to manage and motivate them. An overworked, under-motivated team is unarguably an increased risk.

Conclusion

The organisations responsible for heating and lighting our homes as well as our communications have seen a dramatic increase in the scale of remote working during the global pandemic. This change is likely set for the foreseeable future. As these new working practices become normalised and accepted, it's hard to imagine rolling back to a more traditional office set up post-pandemic.

These changes have been hugely disruptive, and the disruption is being exploited by attackers who are now seeing the remote worker and remote infrastructure as a primary target. Primary because

[6] Post Pandemic Security Planning – Computing Research

many remote workers are distracted by their new environment and more likely to make mistakes, and because some will be working on unsanctioned and unprotected devices. IT teams struggle to prevent this, and do not have the same level of confidence in remote worker/device security as they do in other aspects of their cybersecurity.

Utilities companies also face an onslaught of attacks by virtue of their critical importance in national infrastructure and also because of their increasingly large, distributed, and yet highly connected nature. With bitter irony, it's smartness that makes them vulnerable. One vulnerable endpoint could act as a doorway for an attacker to enact a national meltdown if they chose to bring it about.

The patchy reality of endpoint security and increasing volumes of attacks exploiting the pandemic and remote workers has added weight to the prevailing view that breaches are inevitable, and to the underlying implication that focus needs to be on remediation. The problem is that this remediation is far from straight forward. Greater levels of remote working have increased the burden on already stressed-out SOC/SIEM teams. 13% of contributors had to interrogate between seven and 10 sources of data in the event of a security incident, and 15% had to interrogate more than 10 sources. Many security teams are undermanned and over worked, and their leadership is often finding it harder to manage and motivate them. There are record numbers of vacant cybersecurity posts across all industries and the skills gap is a real and pressing problem for the utilities industry as much as any other.[7]

The picture of escalating attack levels, patchy endpoint protection, and the time-consuming, manual processes for remediation build a case for renewed focus on the endpoint to prevent cybersecurity teams from being overwhelmed. And not just the endpoints owned by the enterprise, but every single one that is being used to access the network, applications, and data – in the cloud or on-premises. It is clearly unrealistic to expect no breaches at all, but stronger defences at the endpoint can significantly reduce the burden on cybersecurity teams and reduce the risks posed to critical national infrastructure and services.

Solutions that sandbox applications and data on personal devices – from phones to laptops – and that secure document collaboration in workers' preferred productivity solutions exist, and can massively reduce the vulnerability of an organisation without compromising the productivity of its remote workers. The same solutions can also encompass IoT and Edge devices, and ensure that these devices are managed and secured to the same standard as other endpoints – no matter where they are.

The next generation of universal endpoint management (UEM) and security solutions have rendered obsolete the idea that security and productivity have to be traded off against each other. The costs of compromised security in an organisation delivering critical infrastructure are high – and potentially extend far beyond financial losses. It's hard to think of another industry to which the strategy of prevention rather than cure is more suited. By placing as much focus on the endpoint as on remediation, next-generation UEM enables utility providers to enact such a strategy.

[7] https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020

About the sponsor, BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 150M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear – to secure a connected future you can trust.

BlackBerry. Intelligent Security. Everywhere.

For more information:

Visit: www.BlackBerry.com and follow @BlackBerry