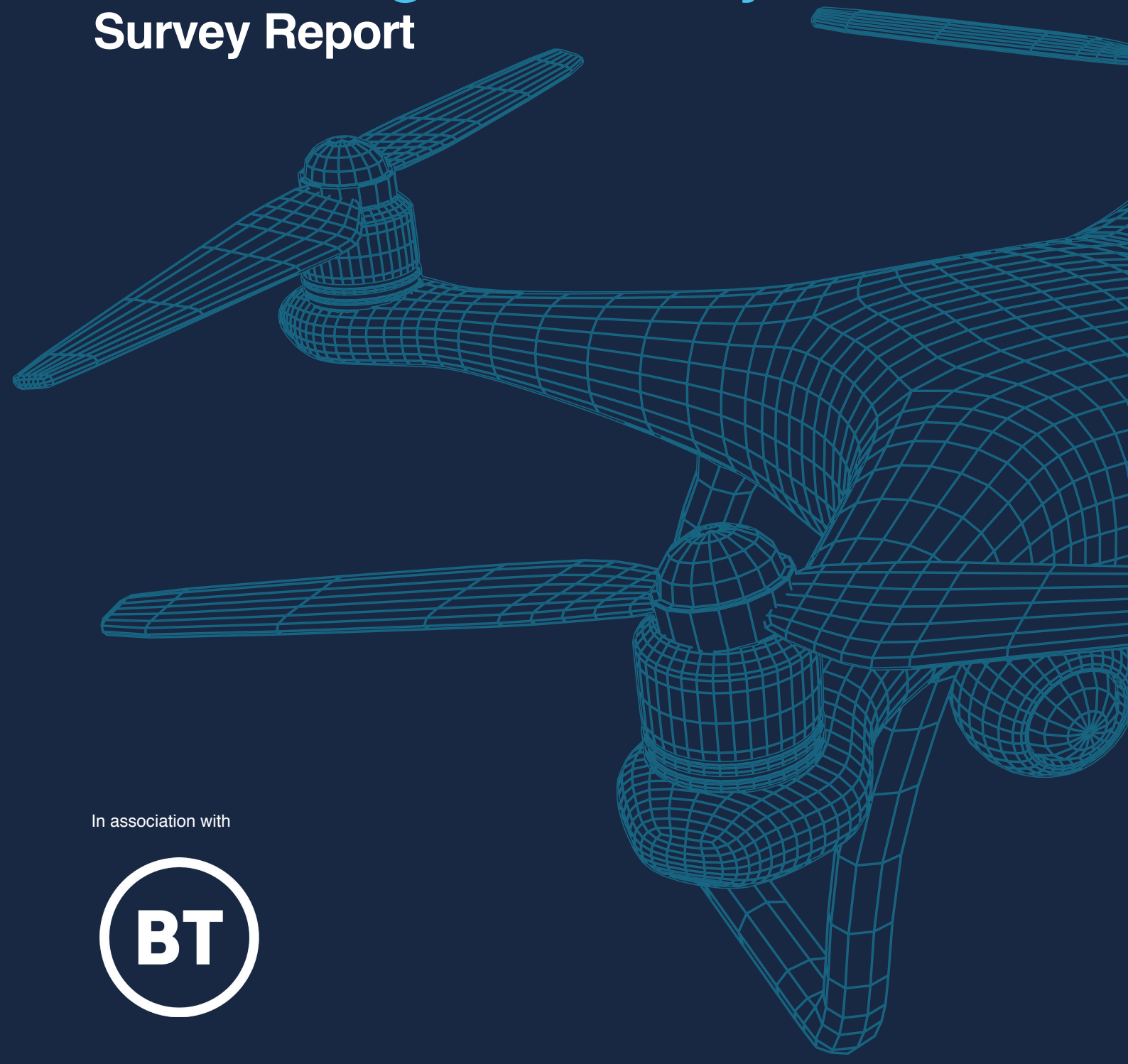
DEFENCE ONLINE

exec survey

Counter Drones: The New Age of Security

Survey Report



In association with

BT

Contents

Introduction

Drones present significant economic opportunities for UK businesses and the public sector. Until recently drones - also known as 'unmanned aircraft vehicles' (UAVs) - had few users outside of specialist military operators and airplane pilots. Today, drones are increasingly available, easy to use, technologically capable, and very affordable. Off-the-shelf drones can be used for leisure and commercial activities, they vary in size and weight, with prices ranging from few hundred to several thousand pounds depending on performance and capabilities.

It is common for drones to be modified and upgraded, particularly by hobbyists and enthusiasts. There is a growing range of positive user cases on drone applications, from aerial photography in film production, surveying, and mapping in agriculture to search and rescue in emergency services. If fully adopted, integrating drone technology into business operations can revolutionise UK industries. From an economic perspective, it can increase business efficiency and save labour costs. While, there is social impact in the removal of physical human presence from dangerous situations.

However, drones can also be used for targeted destruction. A combination of drones and missiles were used to attack Saudi oil production facilities in December 2019. Following the previous year when unplanned drone activity caused severe disruption at Gatwick Airport during the busy Christmas holidays. All of the above highlight the significant threat of rogue drone activity to critical infrastructure and public safety. Closer to home, there are reported cases of organised criminal gangs using drones to smuggle contraband items to inmates at UK prisons. Furthermore, the threat of terrorism via drone attacks to UK national security remains constant. Thus, the Government release of the UK Counter-Unmanned Aircraft Strategy in September 2019 provided the building blocks for a framework to ensure technological innovation is matched with policies on security, regulation, legislation, and education.

On the other hand, the Government cannot shoulder the burden alone, leading them to make the admission that sectors particularly at risk within private industry will have to consider their vulnerability to drone use, and how they should best mitigate it safely and legally. There is clearly need for end-to-end security solutions. The counter-drone industry is relatively small, with few providers able to offer a layered system that is suitable for all situations. It is vital that counter-drone solutions can be tailored to provide a range of capabilities including geo-fences, equipment to detect, track and identify (DTI), and effector equipment that can disrupt illegally operated drones.

As work continues on setting the right legislation for the evolving threat and technological advances in drone technology, industry experts can support the UK Government by providing training and guidance on the risks posed by malicious and illegal drone activities; as well as the positive impact countering the threat of rogue drones can have on privacy, security and public safety.

With this in mind, Exec Survey partnered with Defence Online and the Counter-Drone Solutions team at BT to consider the level of industry awareness posed by illegal or malicious drone activities. The aim of the report is to support organisations with next steps in protecting their employees, customers and key assets from the potential threats of rogue drones.

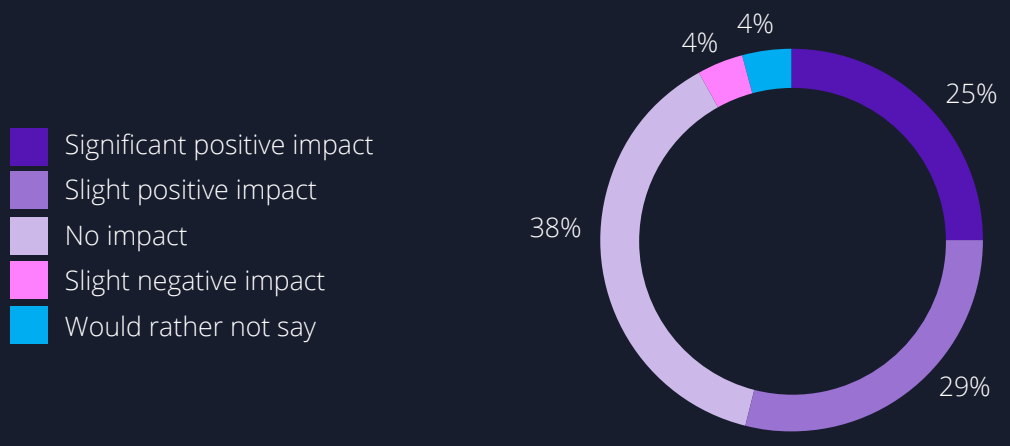
Key Findings

1. A lot of organisations see the benefits and positive impact of drones

The majority of participants in the survey recognise the positive impact and benefits that come with the use of drones, with **54%** of participants believing drones have a positive impact on their organisation.

Over a third **(38%)** feel they have seen no impact upon business, while only **4%** feel that drone technology has caused a slight negative impact.

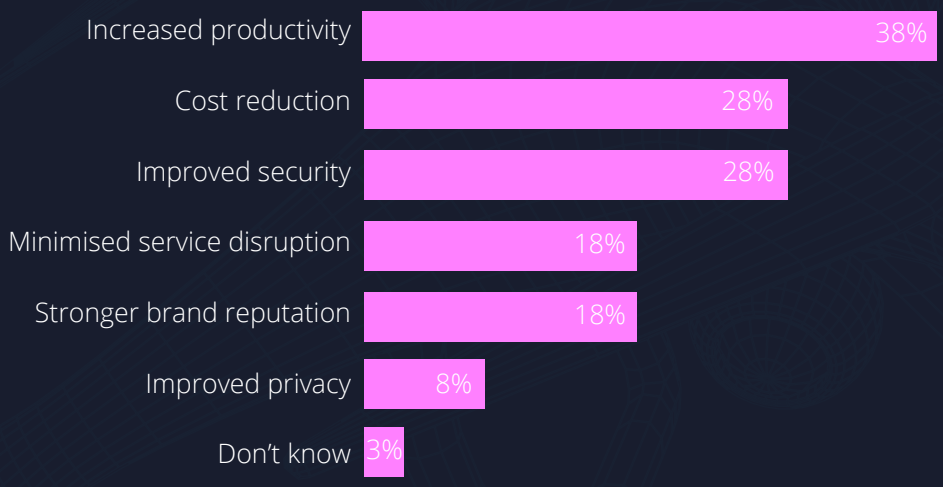
FIGURE 1: Thinking about your industry/sector, how much of an impact do you believe that the rising use of 'drones' has had on your organisation?



For those organisations who are already using drones in business operations, significant benefits have been realised in the shape of increased productivity **(38%)**, improved security **(28%)**, and cost reduction **(28%)**. The results also reveal the numerous benefits that the use of drones can provide.

Anecdotal evidence also pointed to other key positives such as improving safety through drones undertaking potentially dangerous tasks that would previously have been carried out by employees.

FIGURE 2: In your opinion, what positive impact, if any, has your organisation seen from the internal use of drones? Please tick all that apply.

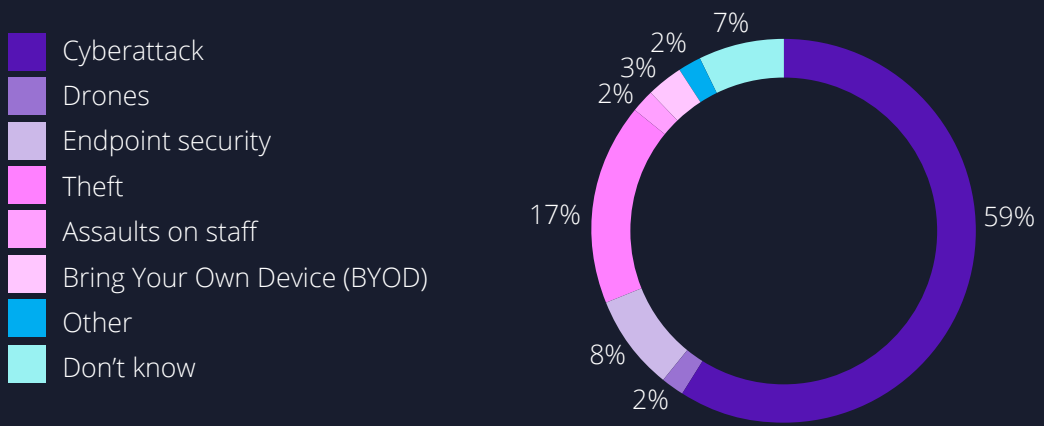


2. Organisations are primarily concerned about cyber security, data theft and invasion of privacy

When considering potential risks to their organisations, almost **60%** cited cyberattacks as their chief concern, with theft some way behind on **17%**. Interestingly, only **2%** recognised drones as the biggest risk or challenge.

This would suggest that the industry isn't aware that unplanned drone activity can also be responsible for carrying out a cyberattack, risking the safety of their customers and employees' data. Further education and creating awareness of these issues should be a priority if organisations are to re-evaluate their perception of the risks posed by drone misuse.

FIGURE 3: When thinking about security threats to your organisation, which of the following areas presents the single biggest risk and/or challenge?



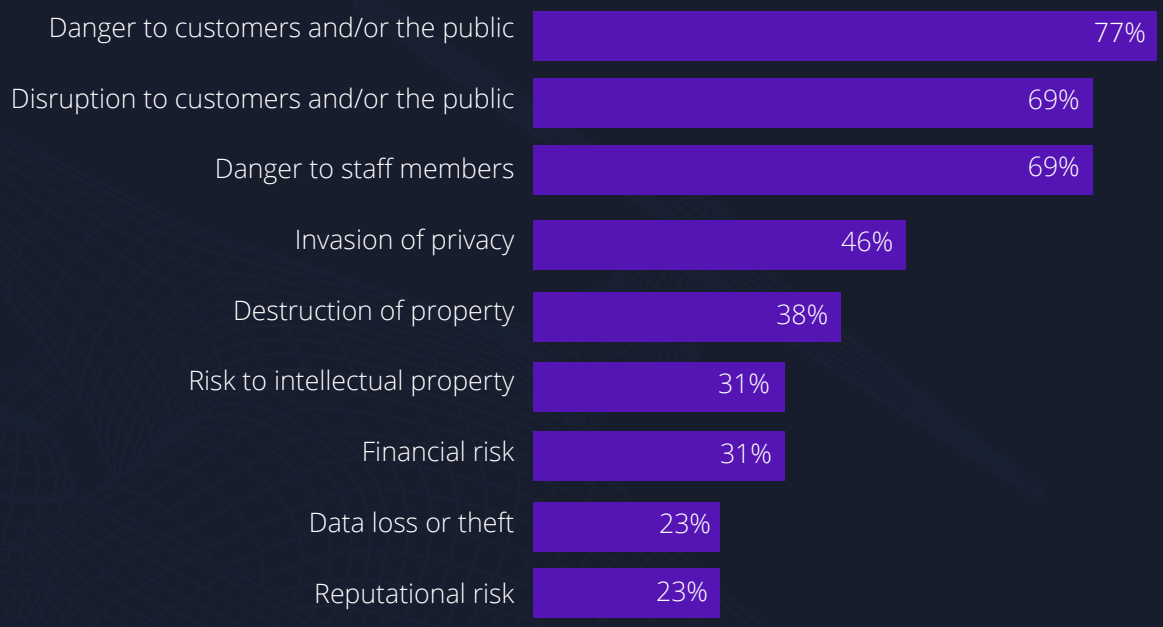
There was, however, recognition of the type of risk that unplanned drone activity could pose to businesses. Perhaps unsurprisingly, for those who view the public use of drones as a significant threat to their organisation, the threat of physical danger to customers and /or the public came out top at **77%**.

This was followed closely by danger to staff members at **69%** and disruption to customers and /or the public, also at **69%**.

The high-profile nature of the disruption and potential consequences caused at UK airports in late 2018 by rogue drones is likely to still be prevalent in many people's minds so it is perhaps unsurprising to see disruption and danger to customers and public safety figure highly.

Invasion of privacy **(46%)** and destruction of property **(38%)** were also flagged as potential threats, pointing to how drones could potentially conduct inspection activities undetected or unnoticed, leaving bad actors plenty of time to prepare for more sophisticated acts of sabotage.

FIGURE 4: In your opinion, what type of threat does unplanned drone activity present to your organisation? Please tick all that apply.



3. Organisations don't realise a counter-drone solution is part of a wider cyber security proposition

The responses to the survey would suggest that businesses don't recognise drones as a threat beyond the physical aspect. Over half **(54%)** don't believe that drones present a threat or nuisance to their organisations.

Risks arising from criminal drone use such as data security or invasion of privacy don't seem to hold the same level of concern as the more publicised cyber scams, for example, phishing or hacking.

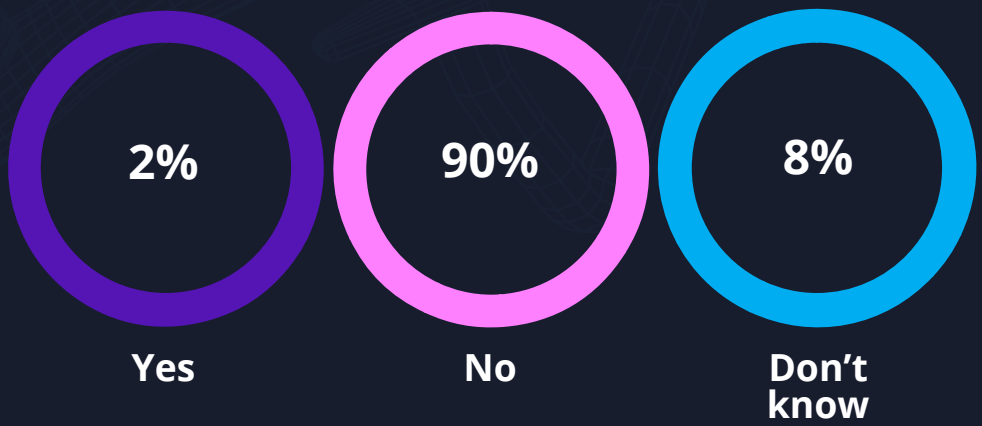
Public awareness of cyber threats via computers or mobile devices is higher; unsurprising given the widespread usage of such devices means people are much more likely to be affected by such attacks, as opposed to attacks targeting drone usage.

Also, the Government has made cyber awareness a priority with frequent campaigns urging businesses to maintain cyber safety in the increasingly digital world.

FIGURE 5: Do you believe that the public use of drones or UAVs presents a threat (i.e. a malicious or criminal risk) or a nuisance (i.e. individuals acting carelessly) to your organisation?

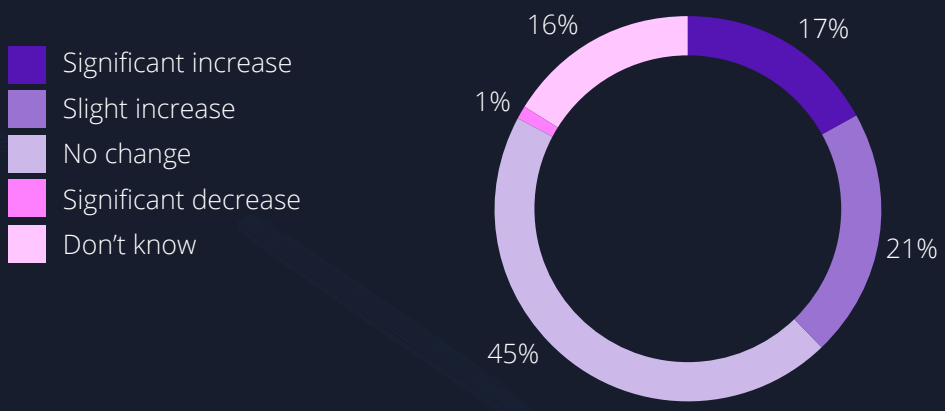
The survey revealed that **90%** hadn't experienced any security breaches arising from drone activity. As the use of drones continues to increase, it is likely that the number of organisations that experience such incidents will also increase.

FIGURE 6: Has your organisation experienced any breaches or incidents resulting from the use of drones against your organisation?



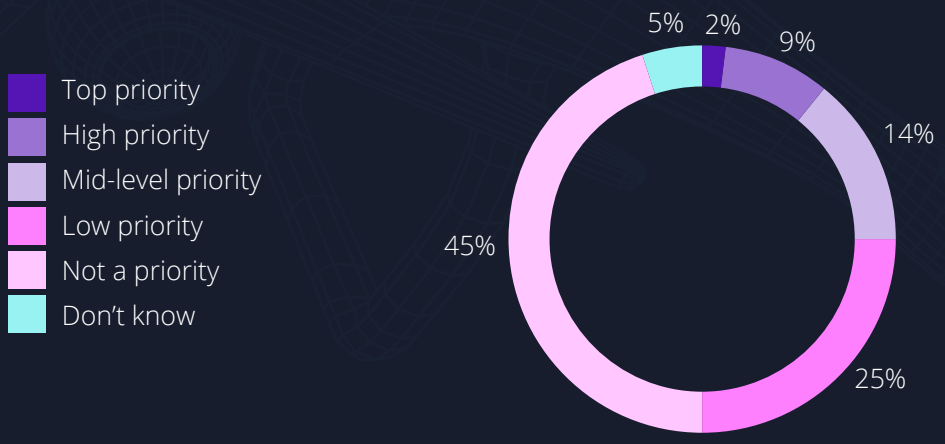
Conversely, there does appear to be some recognition that an increase in the number of incidents will become more likely. A combined **38%** expect to see a rising risk from rogue drone activity. This still leaves **45%** of our survey participants who don't anticipate any change in risk caused by rogue drone use in the future. One challenge is data security risks are mostly seen through the lens of computer hacks, even though, corporate networks can be heavily affected by the malicious use of drones. Companies will need to be made aware why they need to have solid security measures in place to prevent unwanted cyber access and protect themselves from cyber warfare attack.

FIGURE 7: Do you expect rogue drones to become a bigger risk for your organisation in the future?



When understanding the trajectory of innovative technologies, it is often the case individuals and businesses tend to overestimate changes in the near term and underestimate the impact in the long term. The evidence shows that organisations are underestimating the long-term impact of malicious drone activity. The figures show only **2%** view combating the risks posed by drone technology as a top priority and **9%** as a high priority. Furthermore, a combined **65%** see the threat as a low priority or not a priority at all. This is concerning because the UK must position itself as a global leader in the race to cyber security.

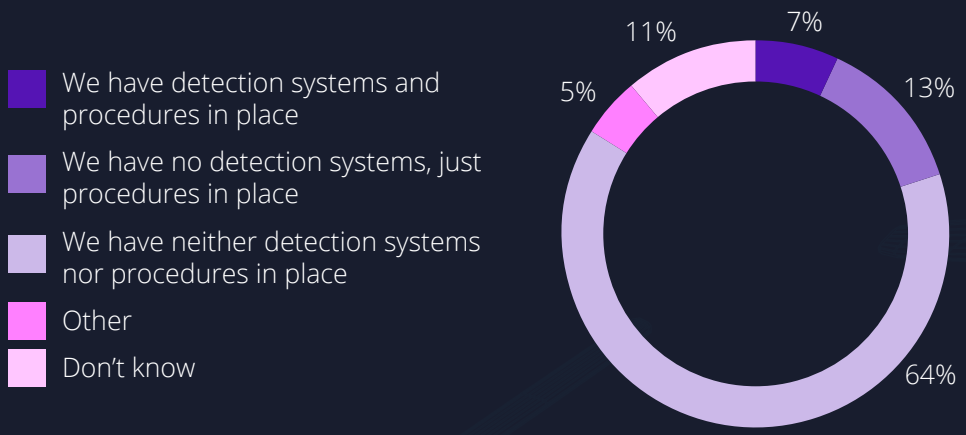
FIGURE 8: How high a priority is combating the risk posed by drones in your organisation?



This is supported by the lack of measures currently implemented to combat the threat of drone misuse. Only **17%** have any form of procedures in place, with only **7%** confirming they operate detection systems.

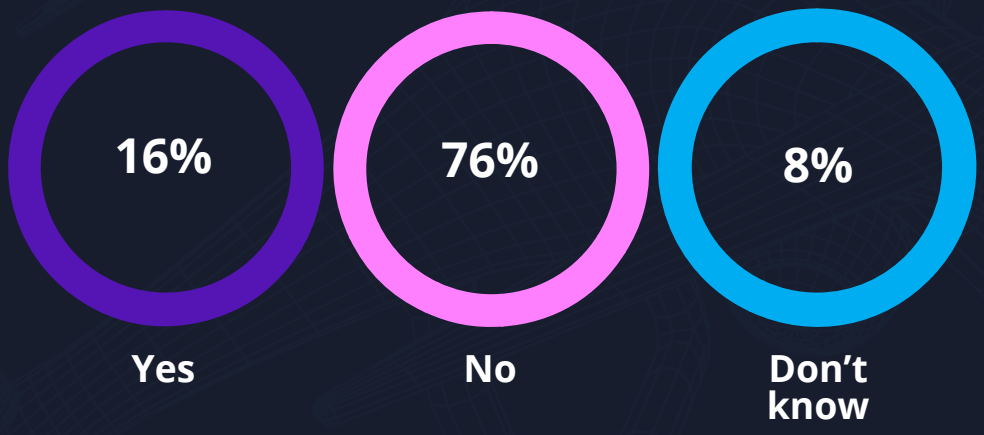
A large majority **(65%)** admitted to having neither detection systems nor procedures in place to deal with an incident of drone misuse.

FIGURE 9: What measures has your organisation implemented to protect against the risk of drones? Please tick all that apply.



Perhaps even more alarmingly, over three quarters of organisations admitted that they don't even have a counter-drone strategy in place. This means that large sections of industry are unprepared and likely, unaware, of the potential damage and disruption a rogue drone could cause to business operations.

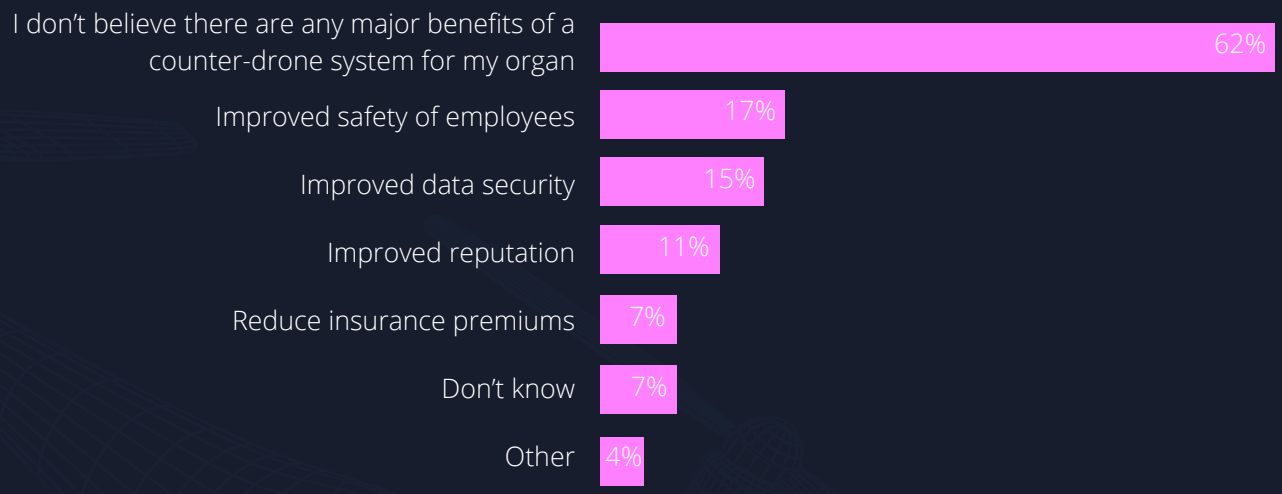
FIGURE 10: Does your organisation have a counter-drone strategy in place?



It stands to reason that private businesses often fail to evaluate the benefits of technologies that have a positive societal impact. In the survey, **62%** of businesses did not see the benefits of implementing a counter-drone system. A potentially dangerous outlook that it can't and won't happen is leaving many organisations vulnerable to a threat that is only going to increase as the use and availability of affordable drones continues to rise.

Of the other responses, there were some benefits identified including improved safety of employees **(17%)**, data security **(15%)**, reputation **(11%)** and a reduction in insurance premiums **(7%)**.

FIGURE 11: Do you feel that there are major benefits to your organisation in adopting or using a counter-drone system? Please tick all that apply.



Examining the reasons why organisations chose not to invest in a counter-drone system further underlined the position that many of them do not consider a counter-drone system a priority **(48%)** and **15%** simply chose not to, despite not facing any barriers to investment.

There was clearly an element of concern about the perceived cost of such an undertaking with **21%** citing that as a reason. Overall , responses demonstrate that the majority of the organisations surveyed are failing to grasp the urgency of implementing an effective counter-drone strategy and system, and it is clear the role education will play going forward is more important than ever.

FIGURE 12: What are the potential barriers to your business investing in a counter-drone system? Please tick all that apply.

Conclusion

By Dave Pankhurst, Head of Drone Solutions at BT

When we launched our Counter-drones solution in September 2019, several existing partners asked; why is BT offering a drone detection and response service? What expertise does BT have in drone technology? Then we explained how our network already protects the UK's critical national infrastructure, including the MOD and GCHQ. We have 4G and 5G in more spots across the nation than ever before, providing higher than 99.9% network availability. We employ over 3,000 cybersecurity experts and ethical hackers who test and protect the network and our customers 24/7, while our BT intelligence team processes and assesses over 2 billion potential threats every hour.

Therefore, we knew that BT could add tremendous value to the revolution in drone technology. We partnered with DroneShield, a world leader in counterdrone solutions, with its DroneSentinel multi-sensor system accredited by UK Government's Centre for Protection of National Infrastructure (CPNI) to offer an enterprise grade network with round the clock support. The high response rate to this report and the wide range of senior level respondents - representing sectors including defence, military, airports, prisons, corporations, critical infrastructure, and events and arenas - have shown there is strong interest in drone technology.

There is clear optimism about the potential payoffs of drone technology, from which 54% of participants have registered positive benefits following implementation into their organisation. The key capability to reduce physical involvement in critical business operations has been associated with higher productivity, better security, and cost savings over the long run. Yet, the findings highlight that 59% of respondents' biggest fear is the threat of a cyber-attack to their organisation. In the last few years, drones have been increasingly weaponised in cyber warfare around the world. Whether it's hackers using drones to steal sensitive company data, disrupt critical business operations or GPS spoofing to crash a drone into another drone, aircraft or critical infrastructure, the threat of malicious drone activity remains a serious risk. Recent attacks on the US and EU energy sector, as well as rumours of potential critical infrastructure targeting, point towards. the threat level only escalating over the foreseeable future.

Therefore, it is imperative that key sectors in the UK, from defence enablers to event organisers, consider their protection to rogue drone activity. BT is a name they can trust, with 75 years of heritage supplying security solutions to the Ministry of Defence, MI5, and the police. We can visit your site, measure the risks and provide a drone vulnerability assessment. This means we can tailor a Counter-Drones package based on your business needs. Our modular approach means that you can scale security solutions as and when the threat level changes, while we can provide ongoing operation support, ensuring that you are always running on the most up-to-date technologies and systems.

If you would like to hear from a BT Counter-drones Expert, please do not hesitate to get in touch with us in one of the following ways:

Tel: 0800 345 7984
Email: counterdronesolutions@bt.com
Web: business.bt.com/solutions/counter-drones/

Acknowledgements

The survey team at Exec Survey would like to take this opportunity to thank all of those who were able to take part in our research, particularly those who found the time to offer additional insights through additional comments. We would also like to thank our survey partners, Defence Online and BT, for their assistance in compiling the questions, scrutinising the responses, and analysing the results.

To contact the Exec Survey team:
Email: **enquiries@execnews.co.uk**
Tel: 0845 094 8567
Address: **FAO Sandra Peet, Pacific House, Pacific Way, Digital Park, Salford Quays, M50 1DR**

Appendix

BT Enterprise is the leading business communication provider in the UK. We connect more than 1m business customers and public sector organisations with our extensive portfolio of communications and IT solutions. We also provide network products and services to communication providers operating in the UK and Republic of Ireland.

This survey was conducted by Exec Survey and Defence Online in partnership with BT. The project ran from 27th March 2020 to 27th April 2020.

Survey respondents represented a broad cross-section of roles across UK businesses. This included: CEO, CTO, Managing Director, Detective Superintendent. Group Technical Director, Operations Director, Sales Director, Head of Commercial, Head of Estates, Head of Technical Services, Head of Marine Operations. Head of Emergency Planning, and Head of Operational Oversight.

There was no inducement to take part in the survey, and BT was not introduced as the survey partner.

The results displayed throughout this report are based on those who fully completed the questionnaire and are displayed as a percentage of this group, unless explicitly stated otherwise.

Question: Thinking about your industry/sector, how much of an impact do you believe that the rising use of 'drones' has had on your organisation? Please tick all that apply.

Answer	Percent
Significant positive impact	25%
Slight positive impact	29%
No impact	38%
Slight negative impact	4%
Don't know	0%
Would rather not say	4%

Question: Does your organisation currently use drone technology?

Answer	Percent
Yes	32%
No	60%
I am not aware of any drone use in our organisation	6%
Don't know	2%

Question: In your opinion, what positive impact, if any, has your organisation seen from the internal use of drones? Please tick all that apply.

Answer	Percent
Improved security	28%
Improved privacy	8%
Cost reduction	38%
Minimised service disruption	18%
Stronger brand reputation	18%
Increased productivity	38%
Other - please specify	41%
Don't know	3%

Question: Do you believe that the public use of drones or UAVs presents a threat (i.e. a malicious or criminal risk) or a nuisance (i.e. individuals acting carelessly) to your organisation?

Answer	Percent
Drones present a significant threat to my organisation	11%
Drones present a nuisance to my organisation	17%
Drones present neither a threat nor a nuisance to my organisation	54%
Other - please specify	12%
Don't know	6%

Question: What type of unmanned aircraft/drone poses the biggest risk to your organisation?

Answer	Percent
Commercial off-the-shelf	62%
Racing drones	0%
Fixed wing drones	0%
Custom made drones	8%
Autonomous non-RF emitting drones	0%
Non-commercial military drones	7%
Other - please specify	15%
Don't know	8%

Question: In your opinion, what type of threat does unplanned drone activity present to your organisation? Please tick all that apply.

Answer	Percent
Invasion of privacy	46%
Data loss or theft	23%
Destruction of property	38%
Danger to staff members	69%
Danger to customers and/or the public	77%
Disruption to customers and/or the public	69%
Risk to intellectual property	31%
Financial risk	31%
Reputational risk	23%
Other - please specify	0%
Don't know	0%

Question: How would you describe the level of nuisance that drones present for your organisation? Please tick all that apply.

Answer	Percent
Invasion of privacy	48%
Data loss or theft	14%
Destruction of property	5%
Danger to staff members	19%
Danger to customers and/or the public	52%
Disruption to customers and/or the public	48%
Risk to intellectual property	10%
Financial risk	14%
Reputational risk	33%
Other - please specify	5%
Don't know	0%

Question: When thinking about security threats to your organisation, which of the following areas presents the single biggest risk and/or challenge?

Answer	Percent
Cyberattack	59%
Drones	2%
Endpoint security	8%
Theft	17%
Assaults on staff	2%
Bring Your Own Device (BYOD)	3%
Other - please specify	2%
Don't know	7%

Question: Has your organisation experienced any breaches or incidents resulting from the use of drones against your organisation?

Answer	Percent
Yes (please give more details below if happy to do so)	2%
No	90%
Don't know	8%

Question: Do you expect rogue drones to become a bigger risk for your organisation in the future?

Answer	Percent
Significant increase	17%
Slight increase	21%
No change	45%
Slight decrease	0%
Significant decrease	1%
Don't know	16%

Question: How high a priority is combating the risk posed by drones in your organisation?

Answer	Percent
Top priority	2%
High priority	9%
Mid-level priority	14%
Low priority	25%
Not a priority	45%
Don't know	5%

Question: Thinking about the security of your organisation when it comes to drones, which type of drone detection and response capability do you feel would be of most use? Please tick all that apply.

Answer	Percent
Portable, hand-held drone detection and response systems for mobile operations, e.g. perimeter patrol	27%
Vehicle based drone detection and response systems for temporary, short-term operations e.g. event or situation based	10%
Fixed drone detection and response systems for regular use, or longer-term operations e.g. critical infrastructure	23%
Other - please specify	8%
Don't know	32%

Question: What measures has your organisation implemented to protect against the risk of drones? Please tick all that apply.

Answer	Percent
We have detection systems and procedures in place	7%
We have no detection systems, just procedures in place	10%
We have neither detection systems nor procedures in place	64%
Other - please specify	5%
Don't know	11%

Question: Does your organisation have a counter-drone strategy in place?

Answer	Percent
Yes	16%
No	76%
Don't know	8%

Question: As part of your strategy, do you currently use or are you looking to implement a counter-drone system?

Answer	Percent
We currently have a system already in place	22%
We are currently testing a system before rolling it out	11%
We are looking to implement a system in the next six months	5%
We are looking to implement a system in the next twelve months	5%
We are looking to implement a system in the next few years	0%
While we are looking into counter-drone technology, we currently have no timeframe for its adoption	33%
Other - please specify	11%
Don't know	11%

Question: Thinking about the use of a counter-drone system in your organisation, who is currently the operator of this system?

Answer	Percent
Inhouse security team	25%
Third-party security team	0%
Specialist Counter-drones team	75%
Police	0%
Cyber security team	0%
ICT team	0%
We're currently looking at changing the operator of our counter-drone system	0%
Other - please specify	0%
Don't know	0%

Grid: On a scale of 1 to 5, where 1 is not at all important and 5 is very important, how important are the following when selecting a counter-drone supplier?

Question: Detection and response capability

Answer	Percent
1	0%
2	0%
3	0%
4	50%
5	50%

Question: Managed service

Answer	Percent
1	25%
2	0%
3	25%
4	25%
5	25%

Question: Cost efficiency

Answer	Percent
1	0%
2	25%
3	50%
4	25%
5	0%

Question: Future proofing

Answer	Percent
1	0%
2	0%
3	0%
4	50%
5	50%

Question: How would you prefer to purchase drone detection and response capability?

Answer	Percent
Upfront, outright purchase	25%
Finance	0%
Lease	50%
Other - please specify	25%
Don't know	0%

Question: Do you feel that there are major benefits to your organisation in adopting or using a counter-drone system? Please tick all that apply.

Answer	Percent
Improved data security	15%
Improved safety of employees	17%
Improved reputation	11%
Reduce insurance premiums	7%
I don't believe there are any major benefits of a counter-drone system for my organisation	62%
Other - please specify	4%
Don't know	7%

Question: What are the potential barriers to your business investing in a counter-drone system? Please tick all that apply.

Answer	Percent
Supplier/solution not approved via commercial frameworks (i.e. CPNI, DSTL)	7%
Perceived cost	21%
Lack of senior management buy-in	12%
Not considered a priority	48%
Unsure about how best to approach	6%
Technology too novel	7%
Doesn't solve my problem (i.e. need more than 'detect only')	6%
Lack of in-house expertise	8%
Risk of liability	5%
Unsure of where to turn for guidance	5%
Lack of resources necessary to adopt	12%
There are no barriers for us	15%
Other - please specify	7%
Don't know	11%

Question: Thinking about the way in which your organisation uses, or would use, a counter-drone system, which of the following functionalities are important to you? Please tick all that apply.

Answer	Percent
Radio frequency detection	22%
Radar detection	19%
Optical and image based detection	21%
Acoustic detection	8%
Altitude tracking	12%
Unmanned Aircraft/Drone identification	26%
Pilot localisation	11%
Reporting and analytics	13%
Forensic evidence gathering	11%
Effector systems	9%
Integration to other platforms/systems	15%
Other - please specify	4%
Don't know	47%

Question: Do you feel the government is doing enough to regulate the use of drones following the release of UK Counter-Unmanned Aircraft Strategy Paper in October 2019?

Answer	Percent
I believe the strategy put in place by the government works to protect individual users and companies from the risks posed by drones	7%
I think the strategy is a good start in regulating the use of drones, however more needs to be done	36%
I don't believe the government's strategy does enough to protect both organisations and drone users	15%
I am not aware of the government's strategy at present	21%
Other - please specify	2%
Don't know	18%

execsurvey

email: enquiries@execsurvey.com tel: 0845 094 9567