Department for Digital, Culture, Media & Sport

Ipsos MORI

Cyber Security Breaches Survey 2021

The Cyber Security Breaches Survey is a quantitative and qualitative study of UK businesses, charities and education institutions. It helps these organisations to understand the nature and significance of the cyber security threats they face, and what others are doing to stay secure. It also supports the government to shape future policy in this area.

For this latest release, the quantitative survey was carried out in winter 2020/21 and the qualitative element in early 2021.

Responsible analyst:

Emma Johns
07990602870

Statistical enquiries:

evidence@dcms.gov.uk
@DCMSinsight

General enquiries:

enquiries@dcms.gov.uk

Media enquiries:

020 7211 2210

Contents

Summary 1
Chapter 1: Introduction 4
1.1 Code of practice for statistics 4
1.2 Background 4
1.3 Methodology 4
1.4 Changes since the 2020 survey 5
1.5 Interpretation of findings 5
1.6 Acknowledgements 6
Chapter 2: Profiling UK businesses and charities 7
2.1 The digital footprint of different organisations 7
2.2 Use of industrial control systems 8
2.3 Use of personal devices 9
2.4 Older versions of Windows 9
Chapter 3: Awareness and attitudes 11
3.1 Perceived importance of cyber security 11
3.2 Involvement of senior management 13
3.3 Sources of information 16
3.4 Cyber security priorities and drivers of change 20
Chapter 4: Approaches to cyber security 22
4.1 Identifying, managing and minimising cyber risks 22
4.2 Insurance against cyber security breaches 27
4.3 Technical cyber security controls 29
4.4 Staff training and awareness raising 31
4.5 Responsibility for cyber security 32
4.6 Outsourcing of cyber security functions 32
4.7 Cyber security policies and other documentation 33
4.8 Cyber accreditations and government initiatives 35
4.9 Dealing with COVID-19 39
Chapter 5: Incidence and impact of breaches or attacks 42
5.1 Identified breaches or attacks 42
5.2 The breaches and attacks considered most disruptive 45
5.3 Frequency of breaches or attacks 46
5.4 How are businesses affected? 47
5.5 Financial cost of breaches or attacks 51
Chapter 6: Dealing with breaches or attacks 56
6.1 Incident response 56
6.2 Reporting breaches or attacks 57
6.3 Actions taken to prevent future breaches or attacks 58
Chapter 7: Conclusions 60
Annex A: Further information 62
Annex B: Guide to statistical reliability 63

Summary

This sixth survey in the annual series continues to show that cyber security breaches are a serious threat to all types of businesses and charities. Among those identifying breaches or attacks, their frequency is undiminished, and phishing remains the most common threat vector.

Four in ten businesses (39%) and a quarter of charities (26%) report having cyber security breaches or attacks in the last 12 months. Like previous years, this is higher among medium businesses (65%), large businesses (64%) and high-income charities (51%).[1]

This year, fewer businesses are identifying breaches or attacks than in 2020 (when it was 46%), while the charity results are unchanged. This could be the result of a reduction in trading activity from businesses during the pandemic, which may have inadvertently made some businesses temporarily less detectable to attackers this year.

However, other quantitative and qualitative evidence from the study suggests that the risk level is potentially higher than ever under COVID-19, and that businesses are finding it harder to administer cyber security measures during the pandemic. For example, fewer businesses are now deploying security monitoring tools (35%, vs. 40% last year) or undertaking any form of user monitoring (32% vs. 38%). Therefore, this reduction among businesses possibly suggests that they are simply less aware than before of the breaches and attacks their staff are facing.

Among those that have identified breaches or attacks, around a quarter (27% of these businesses and 23% of these charities) experience them at least once a week. The most common by far are phishing attacks (for 83% and 79% respectively), followed by impersonation (for 27% and 23%). Broadly, these patterns around frequency and threat vectors are in line with the 2020 and 2019 results.

A sizeable number of organisations that identify breaches report a specific negative outcome or impact. On average, for those that do, the costs are substantial.

Among the 39 per cent of businesses and 26 per cent of charities that identify breaches or attacks, one in five (21% and 18% respectively) end up losing money, data or other assets. One-third of businesses (35%) and four in ten charities (40%) report being negatively impacted regardless, for example because they require new post-breach measures, have staff time diverted or suffer wider business disruption.

These figures have shifted gradually over time – the proportions experiencing negative outcomes or impacts in 2021 are significantly lower than in 2019 and preceding years. This is not due to breaches or attacks becoming less frequent, with no notable change in frequency this year. Instead, it may, in part, be due to more organisations implementing basic cyber security measures following the introduction of the General Data Protection Regulation (GDPR) in 2018. It could also reflect other trends such as the rising use of cloud storage and backups.

Nevertheless, where businesses have faced breaches with material outcomes, the average (mean) cost of all the cyber security breaches these businesses have experienced in the past 12 months is estimated to be £8,460. For medium and large firms combined, this average cost is higher, at £13,400. There are too few charities in the sample to report average costs in this way, but the overall costs recorded for businesses and charities follow a similar pattern.

[1] For businesses, analysis by size splits the population into micro businesses (1 to 9 employees), small businesses (10 to 49 employees), medium businesses (50 to 249 employees) and large businesses (250 employees or more). For charities, we look at annual income bands, with high income being £500,000 or more.

Despite COVID-19 stretching many organisation's cyber security teams to their limits, cyber security remains a priority for management boards. But it has not necessarily become a higher priority under the pandemic

Three-quarters (77%) of businesses say cyber security is a high priority for their directors or senior managers, while seven in ten charities (68%) say this of their trustees. While there have been minor fluctuations in these findings over the past three years, cyber security remains a higher priority compared to when we first surveyed each group (i.e. 69% in 2016 for businesses and 53% in 2018 for charities).

Half of businesses (50%) and four in ten charities (40%) update their senior management teams about the actions taken on cyber security at least quarterly, in line with the 2020 results. However, the percentage of charities reporting that their senior managers are never updated on cyber security has increased since last year (to 23%, vs. 12% in 2020).

Overwhelmingly, businesses (84%) and charities (80%) say COVID-19 has made no change to the importance they place on cyber security. The qualitative research suggests that some organisations have increased their investment in IT and cyber security in response to the pandemic. Many organisations adopted new security solutions, including cloud security and multi-factor authentication, or new rules requiring VPN connections to access files.

These changes were often characterised as being about business and IT service continuity. However, in some cases, interviewees felt that management boards and end users did not fully appreciate the role of cyber security in facilitating long-term business continuity. In the immediacy of the pandemic, cyber security measures were sometimes viewed in the short term as being in conflict with business continuity, rather than complementing it.

The COVID-19 pandemic has led to significant changes in ways of working. This has made cyber security harder for many organisations.

In qualitative interviews, many organisations explained that COVID-19 and the ensuing move to home working initiated substantial changes in their digital infrastructure. Many issued laptops or tablets to staff, set up Virtual Private Networks (VPNs) or expanded existing VPN capacity, started using cloud servers and had to quickly approve new software. In a new question this year, the survey finds that a third of businesses (34%) and a fifth of charities (20%) have a VPN.

These changes have led to new challenges for organisations to contend with, as part of their cyber security management approaches:

- Direct security and user monitoring have become harder in organisations where staff are working remotely. As previously noted, fewer businesses are deploying security monitoring tools than in 2020 (down from 40% to 35%). Fewer businesses (32%, vs. 38% in 2020) and charities (29% vs. 38%) are now undertaking any form of user monitoring.
- Upgrading hardware, software and systems has also become more difficult. With staff working at home, there are more endpoints for organisations to keep track of. Fewer businesses (83%, vs. 88% in 2020) and charities (69% vs. 78%) report having up-to-date malware protection. Fewer businesses (78% vs. 83%) and charities (57% vs. 72%) have set up network firewalls. In large businesses in particular, having laptops with unsupported versions of Windows is a significant security risk (affecting 32% of large businesses).
- More generally, the pandemic had stretched resources and led to competing priorities in IT and cyber security teams. In some cases, there was a perceived conflict between prioritising IT service continuity and maintenance work, and aspects of cyber security such as patching software.

COVID-19 has been an unexpected and unprecedented challenge for organisations. But in terms of cyber security, the findings highlight that there is more they can do to plan for, and ensure they are resilient to, future uncertainties.

The survey findings highlight that a minority of organisations overall have taken actions in the following areas – although they are far more common among medium and large businesses:

- taking out some form of cyber insurance (43% of businesses and 29% of charities) – this is up from 32 per cent for businesses in 2020
- undertaking cyber security risk assessments (34% and 32%)
- testing staff, such as through mock phishing exercises (20% and 14%)
- carrying out cyber security vulnerability audits (15% and 12%)
- reviewing cyber security risks posed by suppliers (12% and 8%).

As the UK emerges from the COVID-19 pandemic, organisations might also consider what more they can do to manage cyber security risks in a "blended" working environment (i.e. where staff are regularly working both in offices and at home):

- Three in ten businesses (31%) and slightly fewer charities (27%) have a business continuity plan that covers cyber security. This was a new question for 2021.
- A quarter of businesses and charities (23% of each) have cyber security policies that cover home working. A fifth of businesses (18%) and a quarter of charities (23%) have policies that cover the use of personal devices for work. The extent to which these areas feature in cyber security policies has not changed significantly since last year.
- Over four in ten businesses (46%) and three in ten charities (30%) are using smart (i.e. network-connected) devices in workplaces. This was also a new question for 2021, and highlights a potential new area of cyber risk for organisations to address.

The qualitative research also highlights organisations' cyber security ambitions for the future and the broader challenges they expect to face. Many expect to make continuous improvements in their cyber security, which includes, for example, rolling out multi-factor authentication, or tweaking policies and processes to cover Software as a Service (SaaS). Some also expect to move further away from an approach of locking down user activity, towards one that prioritises functionality and flexibility. Cyber security teams may therefore need to realign themselves to wider strategic business needs in some cases, emphasising how staff can use new technologies, software and platforms securely rather than banning them.