March 2021

Cyber and Gambling

Cyber security in the gambling and lottery sector

Dorothee Stellmacher, Hannah Shrimpton, Edward Camilleri

Ipsos MORI

Contents

1 Executive Summary

The **National Cyber Security Centre (NCSC)** commissioned **Ipsos MORI** to conduct a mixed-method study into **cyber security practices within the gambling and lottery sector in the UK.**

Key findings set out in this report include:

- **Attitudes towards cyber security: Stakeholders generally felt that cyber security is an important function and a high priority within the UK gambling and lottery sector.**
  - However, some stakeholders felt that cyber security was not always seen as important as commercial priorities. Having board-level buy-in was seen as key to instilling a more deep-rooted cyber security mind-set across organisations.
  - Stakeholders generally felt they had the right employees and skills within their organisation but acknowledged the sector-wide difficulties around recruitment and retention of staff.
  - Stakeholders did not feel that gender diversity has been achieved within the sector. This was felt to be due to a combination of a general lack of women within tech/IT as well as the sector being very male dominated.
- **Threat overview: The majority of stakeholders indicated they suffered some kind of cyber incident within the last 12-months** but none of the attacks were seen as substantial or as having long-term impacts on their organisations.
  - The Coronavirus (COVID-19) pandemic led to a temporary increase in attacks in early 2020 but stakeholders did not feel that it altered overall threat levels.
  - The most commonly reported attacks were: credential stuffing, DDoS and phishing attacks. Stakeholders flagged ransomware as a key threat to the sector, with attacks becoming more sophisticated and targeted.
- **Preparedness: Stakeholders overall felt well prepared to deal with cyber attacks and felt that employee awareness and knowledge of cyber security was good.** This seems to be the result of ongoing training and awareness raising efforts as well as the development of easy-to-use reporting tools.
  - Cyber security insurance was seen as a useful tool in protecting their organisation against financial harm caused by cyber attacks.
- **Third party and supply chain management: Most of the organisations relied heavily on a number of third-parties**, especially if the underlying betting or gaming services are delivered by third parties, although some tried to limit their reliance by keeping as much as possible in house.
  - Stakeholders were aware of third-party risks and cited a number of controls their organisations had in place to mitigate against them. There were mixed views regarding the levels of awareness among senior management of the risks associated with third parties.
  - Third party controls usually did not extend to fourth parties or the supply chain.

2 Introduction

Overview

The **National Cyber Security Centre (NCSC) commissioned Ipsos MORI** to conduct a mixed-method study into **cyber security practices within the gambling and lottery sector in the UK**. Fieldwork was conducted in February – March 2021 and consisted of 1-hour in-depth telephone **interviews with eight senior cyber security professionals** from some of the largest gambling and lottery organisations, as well as an **online survey**.

Background

The UK gambling sector is worth over £14 billion and employs over 46,000 people; in total contributing £2.3 billion towards the UK GDP[1]. Gambling is a common leisure activity with around 32% of the population gambling weekly and in 2018, there were 36.6 million active customers on web-based betting sites. However, the sector comes with its unique problems and associated risks especially around addiction; in 2019/20, there were over 280,000 problem gamblers identified but only 3% were said to be getting treatment or help[2]. Furthermore, as more of the industry's commerce is conducted online (currently around £4.7 billion of the overall gross gaming yield comes from online gambling[3]) the risk of cyber crime has increased. **The research undertaken by Ipsos MORI will inform how the gambling and lottery sector is protecting itself against cyber crime**.

Objectives

The overarching objective for this research is to explore **the UK gambling and lottery industries key cyber threats and how it deals with cyber security**.

Methodology and sample

Qualitative insights were collected from in-depth interviews with Chief Information Security Officers (CISOs) and other senior level executives responsible for the development and implementation of cyber security measures. This was supplemented by quantitative data from an open-link online survey that was pushed out via the Gambling Commission and other industry bodies[4].

The report will focus predominantly on findings from the qualitative interviews.

[1] https://www.statista.com/topics/3400/gambling-industry-in-the-united-kingdom-uk/
[2] https://www.begambleaware.org/media/2289/annual-stats-2019-20.pdf
[3] https://www.itgovernance.co.uk/gambling-cyber security
[4] Please note that due to the overall small sample of nine respondents, findings from the online survey can only be reported as fractions and are indicative only.

3 Attitudes towards cyber security

Importance of cyber security

The majority of stakeholders saw cyber security as a **very important function** within their organisation as they felt it directly affected their customers' trust and confidence in their services. The fact that the sector is highly regulated in the UK also seemed to help place additional importance on cyber security.

In addition, stakeholders all agreed that cyber security was a **high priority** for their organisation[5]. However, it was recognised that cyber security is often a competing priority, rather than "the only" priority. Some stakeholders felt that cyber security was still seen as part of IT rather than being integral to the overall success of the business.

Similarly, for a small number of stakeholders, the importance placed on cyber security within their organisation felt somewhat superficial and that was down to the internal cyber security teams to keep pushing its importance. Having not just senior, but board level buy-in was seen as key to installing a cyber security mind-set that goes beyond compliance.

> ***"I'd say 2.5 [out of 5]. I'd say superficially speaking it's a 5, it's always a 5, [...] until you start to tell them [senior management] that that priority means you're going to work on this thing [minimising risks] as opposed to delivery on the product."***
> *Cyber security lead, UK based gambling provider*

Ability to protect the organisation

Stakeholders taking part in the interviews all felt they currently had the **right employees with the right skill sets** to help protect their organisations. That being said, stakeholders acknowledged what seemed to be common challenges in recruiting cyber professionals. There was a strong sense that turnover rates are high and the competition for employees has become fiercer as the sector has started to place more importance on cyber security, with rapidly increasing salaries.

One stakeholder also felt that Europe lagged behind the US in its supply of cyber security personnel and companies struggle to convince potential employees to move over to Europe.

Diversity within the sector

It appears that the **proportion of women within the sector remains low**. The highest number mentioned by any participant was 31%. Of those who responded on the online survey, four of the nine participants said 0-10% of their cyber security team identified as a woman.

Most interviewees said it **was important to have gender diversity i**n cyber security. However, there was an acknowledgment that improving diversity can be challenging. One participant expressed the difficulty of hiring from a small resourcing pool of women. As the industry as a whole, and the career paths involved, are generally male-dominated industry, it was felt that diversity needed to start earlier; with encouraging younger women to get into the industry.

[5] This was supported by findings from the survey where all respondents selected cyber security either as a 'fairly or very high priority'.

> ***"[The] gambling sector is very male orientated anyway, so getting women that want to work for a gambling organisation and also are interested in cyber security, there's not that many people around that would want to sit in such a male-dominated department in a male-dominated industry. A lot of women they don't really want to work in that sort of organisation.... You try and address it by numbers, where really you need to make sure that the younger people are interested and they can grow the skills there, because you can't force people to want to work in IT."***
> *Cyber security lead, UK based betting provider*

It is important to note that not everyone agreed on the importance of diversity; some stakeholders felt it was more about having the right people with the right skills rather than gender diversity.

4 Threat overview

Perceived levels of threat

The **perceived level of threat from cyber attacks to gambling and betting organisations was mixed**; while the majority indicated their organisation had suffered some kind of cyber incident in the past 12-months, none of the attacks were seen as substantial. Recent incidents mentioned by the stakeholders all involved low-level credential stuffing or privacy related incidents and distributed denial-of-service (DDoS) attacks that were part of mass campaigns.

The results from the online survey paint an even more mixed picture, with equal proportions indicating no incidents and between 10-100 incidents in the past 12-months. Overall, five out of nine respondents claim they suffered some incidents in the last year, while four out of nine did not experience any incidents or were not aware of any. This seems to be broadly in line with incident levels across general UK business in 2020[6].

Some stakeholders did indicate an increase in attacks over the past year, especially at the beginning of the Covid-19 pandemic. However, stakeholders generally felt that the overall threat level to organisations in the UK gambling and betting sector had **remained the same regardless of the pandemic**. That being said, there was a strong sense that attacks are constantly evolving and becoming more targeted – especially in regard to ransomware (see below):

> ***"I don't think the overall level of threat has changed. I think it's moved on. I think it's become more of a challenge to organisations that didn't have the technical architecture and setup for remote working. We de-scoped what we did, so it wasn't so much of a challenge for us. I think the general threat's moved on, as it always does, regardless of the pandemic. I think ransomware attacks are more problematic now than they were 12 months ago for sure [..] other things have been pretty static."***
> *Cyber security lead, UK based gambling provider*

Of those survey respondents who experienced a recent cyber attack, all reported they had experienced hacking or attempted hacking of online user accounts as well as attacks to take down their website, applications or online services. This was closely followed by computers becoming infected with other viruses, spyware or malware and staff receiving fraudulent emails, voice calls or text messages.

Key threats to the sector

4.1 Credential stuffing

Credential stuffing describes a cyber attack by which hackers use fraudulently gained valid combinations such as username and password from one compromised site to access other sites. The primary motivation behind credential stuffing is usually financial.

Credential stuffing appears to be the most prominent and commonplace cyber attack experienced by IT professionals within the gambling and lottery sector but – similar to DDoS (below) – tends to be seen as

[6] According to the DCMS 2020 Cyber Breaches survey, almost half of businesses (46%) report having cyber security breaches or attacks in the last 12 months. Like previous years, this is higher among medium businesses (68%) and large businesses (75%). https://www.gov.uk/government/statistics/cyber security-breaches-survey-2020/cyber security-breaches-survey-2020

having only limited impact on the organisation at large. The key concern stakeholders held about credential stuffing was around reputational damage if service user's details are compromised.

> ***"It's not like it's [credential stuffing] cost-neutral, but in the grand scheme of things, it's pretty negligible, direct financial cost, even though it's clearly an impact on the player concerned."***
> *Cyber security lead, UK based gambling provider*

4.2 DDoS attacks

DDoS describes a cyber attack designed to render the targeted service inaccessible to users. In the gaming and betting sector this would translate into users being unable to play games online or place bets while a DDoS attack is under way. The primary motivation behind DDoS attacks is usually to create reputational damage to a site but can also be financial when combined with request for payment to end the attacks.

DDoS was mentioned frequently in the interviews, and it seems that the Covid-19 pandemic led to an increase in attacks in early 2020 driven by a combination of boredom and opportunisms.

While cited as a frequent occurrence within the sector, the impact of DDoS was seen as limited to additional staff time required to end the attacks. Although as one stakeholder pointed out that "any incident that requires remediation actions is always going have an impact on delivery."

> ***"There was a 600% increase in incidents that we experienced for about 6-8 week period. That was quite a lot of extra work for my team, we didn't have any issues working from home, everyone's been great, but just that increase in workload was quite a lot for a short period of time, but it's all calmed down since. I do think when it first happened, there was obviously a lot of interest, and people were testing out whether people had the same controls when people were working from home as they were in the office, so we've been quite lucky in that respect."***
> *Cyber security lead, UK based betting provider*

4.3 Phishing

Phishing describes a type of social engineering where attackers trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website.

Phishing can be conducted via a text message, social media, or by phone, but is mainly used to describe attacks that arrive by email.

While mentioned as a frequent type of attack, stakeholders overall felt that their organisations had controls and processes in place to deal with phishing attacks, putting them in a good position to deal with additional challenges such as remote working:

"Phishing [is the biggest threat], although we do have very good controls in place, obviously it relies on a human. If someone is going to click on that link or enter their credentials, there's only so much monitoring we can put in place, so we have had accounts, Office 365 accounts become compromised, and it's then once that compromise has happened, how much further they can get in the organisation just by compromising further accounts. So, I think that's probably our biggest issue really."
Cyber security lead, UK based betting provider

"The best thing we did was we employed a report phishing button, and when people were receiving external mail in the subject, it tags it with external and then just general awareness around, please if you see something report it, even if you, we get a lot of mis-reports that are just spam or whatever, but I'd much rather them over-report than not report that one."
Cyber security lead, UK based betting provider

4.4 Ransomware

Ransomware describes a type of malware that prevents individuals or organisations from accessing their computer. Attackers will then usually ask for a payment to them in order to unlock the affected computer.

While ransomware was not as frequently mentioned as other types of attacks, stakeholders voiced concerns that it presents the **most severe threat to organisations**; both in terms of ability to defend themselves against a possible attack and in terms of potential impact. Some stakeholders reported that ransomware attacks had become more targeted, better planned and more aggressive in their demands for pay-out.

"I think the sophistication is notably different to 12 months ago. Attacks are harder to detect than they were. The higher-end attacks, things like less commodity attacks are more thought through and planned. And I think people have realised that some companies are paying up and so, there's a lower barrier to entry than other types of attacks and frauds. And it can all be done remotely."
Cyber security lead, UK based gambling provider

"The evolution of ransomware is extremely troubling and the abilities of groups like Ryuk, are phenomenally forward-thinking. So, it's an area of great concern […] the level of catastrophe that can occur as an outcome of being compromised if you're targeted by one of these groups. And if you follow the timeline of their attacks to some of the targets that they had, the speed with which they're able to accomplish their tasks was phenomenal, and the ability, even if you had an extremely strong set of controls and proactive CCERT or SOC internally that was able to identify and start to interdict, it's too late [..] you are at their whim once they've done their job. They probably extracted phenomenal amounts of data and they've also encrypted your data so there's no real way out of it even if you're paying the ransoms to unlock it all. So yes, extremely troubling, it's not the same as it was 5 years ago, it is extremely targeted, professional, fast and devastating."
Cyber security lead, UK Online gambling operator

4.5 Other sector specific threats

A small number of stakeholders also mentioned the threat of game manipulation and insider-enabled attacks. Both were seen as potentially damaging to the reputation of the service provider, but neither had occurred against the organisations of the stakeholders we spoke to in the past 12-months.

Impact of attacks

Overall, stakeholders felt that the **impact of cyber attacks experienced in the last year – especially in financial terms – was quite limited**; while the majority of interviewed organisations did experience a number of incidents, recent attacks were mostly seen as low-level attacks which could be fought off with pre-existing controls and mitigation strategies.

When thinking about the potential impact of a successful attack, the key concern voiced by stakeholders was around **loss of reputation**. This was particularly pertinent for public organisations who felt a strong responsibility, not only towards their customers, but also their shareholders. This was heightened by the feeling that the public perception of the gambling and lottery sector is inherently low:

> ***"Had the attacks been successful, it would have impacted the reputation of the company. That would have had a substantial impact, where we'd have to pay some losses as a result of that. In certain cases, we would have had to go out to customers, let them know that something had happened with the account, for instance. So, had the attacks been successful, it would have had a substantial impact on our organisation."***
> Cyber security lead, *UK based betting and gambling provider*

> ***"[…] in the gambling industry. […], we're never starting from the moral high ground, in the gambling industry. So, people have a low opinion, anything bad happens, it's us that are going to get the blame for it."***
> *Cyber security lead, UK based betting provider*

Future threats

Survey respondents were asked about key threats to the betting and gambling sector in the next 2-3 years. Predictions were very varied and included:

- Increasing level and sophistication of cyber security attacks;
- Manipulation of gaming outcomes;
- Insider attacks;
- Intrusion attacks;
- Employees subjected to a greater amount of social engineering/phishing as part of simplifying the infiltration/exploitation of the organisation;
- Attacks on external systems such as finance and payment systems;
- Financial/ organised crime actors targeting the sector through hacking or malware with an emphasis on ransomware;
- Threat actors will hone in on containerised/cloud infrastructure;
- DDoS bitcoin extortion and credential stuffing will continue to be prolific but as equally unsuccessful;
- Threat actors developing more advanced attack tactics e.g. using Internet of Things (IoT) to increase DDoS attacks or Artificial Intelligence (AI) via verified accounts;
- Changes in gambling regulatory framework/ regulatory headwinds;
- Data loss.

5 Levels of preparedness

Overall levels of preparedness

Overall, stakeholders felt **well prepared to deal with cyber attacks**. There was a strong sense that - as organisations with a big online presence and well equipped and dedicated cyber security teams - they were in a good position to protect themselves against cyber attacks and effectively deal with any ongoing incidents. This finding is supported by the result from the online survey, where the majority of respondents (8 out of 9) agree[7] that their organisation has sufficient preventative, detective and corrective controls in place to help protect, mitigate and respond to cyber attacks.

The key challenges for preparedness raised by stakeholders were around ensuring that cyber security was taken into **consideration at every step of the product development**, as well as ensuring that there is better ownership of risks across the board:

> ***"I think we're very good at identifying risks, the architecture team are very good at highlighting risks and so are the Operational Team, the issue is the ownership of those risks and making sure they're either accepted because they're within our risk appetite or we're working on resolving them. So, because people have so many product features to develop, sometimes the security parts, the lower-risk security things don't get worked on. So, it's about making sure the people that own those risks understand them and get their teams working on them, I think that's where we need to focus on."***
> *Cyber security lead, UK based betting provider*

Stakeholders also raised the unique challenges around being prepared to deal with cyber attacks during the COVID-19 pandemic, with large proportions of the workforce working from home on a regular basis. However, stakeholders predominantly felt their organisations had been able to react to the new circumstances quickly and efficiently; even if they had had limited prior experience of mass remote working. Stakeholders predominately felt that their organisations already had effective measures in place to address risks associated with remote working, such as specific employee awareness training or having a Virtual Private Network (VPN).

> ***"We relied on the office as a secure environment, so we've had to make a lot of concessions very quickly, to allow people to freely work from home. Over the past year we've been adapting the controls, so now we have good confidence [that we are] protecting those employees that are working out there instead of in the office."***
> *Cyber security lead, UK based betting and gambling provider*

Employee awareness and knowledge of cyber security

When asked about the awareness and knowledge of all employees (including those not directly involved with cyber security) to identify, respond and report cyber security threat or incident; stakeholders and survey respondents alike agreed that they were **generally well equipped to deal with cyber security threats**. Most of the organisations we spoke to for the qualitative research reported that their organisations had spent substantial time and effort raising cross-company awareness of cyber security risks and educating employees on how to protect themselves. Many of the organisations used a mix of (mandatory) training courses as well as fictitious phishing campaigns to test and improve the resilience

[7] Based on Top-Two-Box measure of "Strongly" and "Tend to" agree

of the wider workforce. There was also an emphasis on communicating those findings across the organisation in order to create buy-in and creating reporting tools that are quick and easy to use.

There was consensus among stakeholders that a top-down approach to cyber security i.e. where cyber security is implemented and promoted from the top is crucial in creating a cyber security mind-set:

> ***"The biggest thing is incorporating it through top-down management, and that's the hardest thing to achieve [...]. Everything else apart from that, the softer skills of just making sure you don't click on emails, everything else, I think it's an important component but it's not integral."***
> *Cyber security lead, UK Online gambling operator*

Within the qualitative sample, organisations that started out as tech start-ups were more likely to say that their senior leadership teams were fully aligned on cyber security.

Value of cyber security insurances

Feelings were **mixed about the value of cyber security insurances**. The majority of interviewed organisations already had a policy to transfer some of their cyber security risks or were currently considering it. The main reasons organisations used a cyber security insurance policy was for financial protection and to provide reassurance to their shareholders and customers.

> ***"We do it because we're a publicly traded company. We owe it to our shareholders, it's not an option. From a practical perspective, I think it's good. As the threats are growing, cyber security, it's all about risk management, you can never protect everything at all times. So, sometimes you'll fail. Having cyber security insurance is a good fall-back mechanism for your key risks, so I think they're useful."***
> *Cyber security lead, UK based betting and gambling provider*

However, in line with findings from the online survey[8], views differed on the usefulness of the policies. Stakeholders generally felt that insurance policies were useful in protecting the organisation against financial risk but not against other risks such as loss of reputation:

> ***"[The cyber security] insurance protects against financial risk, we had penalties from ISPs, from our DNS provider, we were getting penalties for burst charges, there was loss of revenue, there were all these other things that we had to cover, so we got a percentage of that money back through insurance, but it's not protecting against any of the other kinds of risk. It doesn't solve any of the reputational risk or that kind of thing...We'll be the ones in the headline."***
> *Cyber security lead, UK based betting provider*

In addition, some stakeholders also felt that in order to get the most out of the insurance policy, the organisation had to spend substantial time and resource reviewing the policy and ensuring that it would provide adequate cover in case of a breach.

[8] 7 out of 9 respondents selected they either had a cyber security insurance in place or were considering it

6 Third party & supply chain management

Reliance of third parties

All of the organisations taking part in the research reported **using a large number of third parties in order to provide their services**, ranging from approx. 75 to 10,000.

However, stakeholders **differed in their opinions of how reliant their organisations are** on third parties, which was also reflected in the survey responses. Organisations that host a lot of third party games and betting services felt they are quite heavily reliant on those suppliers, as the majority of their customer content comes from third parties. Other organisations tried to limit their reliance of suppliers by keeping as much of their development efforts in house as possible.

> ***"In this industry, a lot of the underlying games themselves are delivered from third parties. We apply brands on top of that. We obviously develop some platforms ourselves to do games, but a lot of it is relying on those third parties. It creates a difficult position because there is a level of monopolisation there. I mean, obviously you have to rely on these particular people. When you're relying on somebody that has much leverage that reduces your ability to start to demand controls or access to data or right to audit and things like that."***
> *Cyber security lead, UK Online gambling operator*

> ***"As an organisation, we try to do as much as we can in-house. If all of our suppliers disappeared, it would have an impact of maybe 30% of our business, but that's about it."***
> *Cyber security lead, UK Online gambling operator*

Key risks associated with third parties

There were a number of key risks associated with third parties. Main concerns raised by stakeholders were around the confidentiality of user data, as well as the possibility for cyber attacks on their own organisation if a third-party product or service was compromised.

Stakeholders also flagged that, in the wake of the SolarWinds hack (see below), large providers are often not seen as suppliers and are therefore not always vetted by their organisation in the same way smaller organisations might be.

There were mixed views on how aware senior management can be about risks posed by third parties. While some stakeholders felt that widely publicised attacks such as the SolarWinds incident helped to raise awareness of third party risks, the overarching feeling was that senior managers tend to be more focused on commercial aspects and compliance than mitigation of risk:

> ***"[Risks posed by third parties/ supply chains] it's talked a lot about [..] in industry about supply-chain risk and also just in the public media after Solar Winds and other examples, where it's a big issue for business. And when it gets talked about a lot in industry, that tends to help us raise-, senior management tend to become aware of their own back anyway without us promoting it as a challenge [..]. We've had internal audits specifically focussed on it from our internal audit function. There's been specific conversations about it at the board level [..] I think the challenge we've got, as do others [...] is that it's [audits are] great for compliance but it's not really mitigating risks."***
> *Cyber security lead, UK based gambling provider*

That being said, stakeholders generally felt they had the right level of support from their senior management teams and sufficient resources to minimise third party risks, especially in relation to governance and compliance.

Mitigating strategies

Stakeholders reported that their organisations use a range of different controls to manage third party risk including:

- Risk assessments
- Contract implementation
- Contract review / renewal or termination
- Corrective actions tracking
- Third party self-assessments
- Performance and compliance reviews, and
- On-boarding processes

The main reasons for implementing these third party controls were: financial (protecting against fines) and as reputational.

Where providers fall under the remit of the Gambling Commission[9] and have to adhere to the same regulations, this was seen as positive, as it provides the organisation with a level of confidence in regard to third party conduct.

Key barriers

The key challenges to implementing third-party controls mentioned by participants included: the sheer volume of suppliers; lack of transparency from suppliers; lack of enforceability; and time/ costs associated with assessing third parties:

> ***"[We] can't do on-site audits for everybody, so we have to get a level of assurance from them and we have to take them at their word for certain things, so that's difficult."***
> *Cyber security lead, UK based betting provider*

There was also a sense that "traditional approaches to third party risk management" were good for compliance, but are unable to fully mitigate supply chain risk.

[9] https://www.gamblingcommission.gov.uk/home.aspx

SolarWinds hack

In early 2020, hackers manged to break into US based SolarWind's software system called "Orion", a system that is widely used by companies across the globe to manage their IT resources. The attackers were able to add a malicious code to the software updates which was sent out by SolarWinds and offered the hackers a backdoor to customer's information technology systems. The hackers then used this backdoor to install more malware and we able to infiltrate up to 200 private companies as well as US Government Departments.

The cyber attack on SolarWinds was frequently mentioned by stakeholders as an example of the limitations of third party controls. Although many organisations felt that they had decent controls in place to limit their risk exposure through third parties, these tend to apply to smaller, less established organisations than their own but do not extend to products or services purchased from well-established providers such as SolarWinds or Microsoft. The main reason behind this was that stakeholders felt that they had little or no control in assessing these products.

> ***"[...] if we look at the Solar Winds breach, they would never have featured as a supplier, they wouldn't, that's a whole different thing. We don't go doing third party assessments on Microsoft if they give us Word for example, it's just that kind of thing doesn't, you go and buy an off-the-shelf product, we don't really count them as a supplier, they aren't counted as a supplier."***
> *Cyber security lead, UK based betting provider*

Fourth party controls

Controls very rarely extended beyond third party agreements. The main reason for this was the lack of (contractual) relationship with fourth parties and the wider supply chain, as well as a lack of enforceability. Stakeholders also did not see it as their responsibility to audit fourth parties, but rather as the responsibility of the third party to implement their own controls.

The only mitigating factors mentioned were contractual clauses with third parties, obliging them to inform the organisation if they intend to outsource any of their services, as well as ensuring that third parties use a range of different suppliers to minimise risk:

> ***"We don't really audit fourth parties in the same way that we audit third parties but we do look for systemic risks. What I mean by that is are we putting all our eggs in 1 basket? Do we think we've spread the risk with 5 third parties, but actually they're all using the same fourth party? Actually, if the fourth party goes down, then our cyber resilience is shot. So, we do do some stuff but it's not as mature as our third party coverage."***
> *Cyber security lead, UK based gambling provider*

End of report

Our standards and accreditations

Ipsos MORI's standards and accreditations provide our clients with the peace of mind that they can always depend on us to deliver reliable, sustainable findings. Our focus on quality and continuous improvement means we have embedded a "right first time" approach throughout our organisation.

ISO 20252

This is the international market research specific standard that supersedes BS 7911/MRQSA and incorporates IQCS (Interviewer Quality Control Scheme). It covers the five stages of a Market Research project. Ipsos MORI was the first company in the world to gain this accreditation.

Market Research Society (MRS) Company Partnership

By being an MRS Company Partner, Ipsos MORI endorses and supports the core MRS brand values of professionalism, research excellence and business effectiveness, and commits to comply with the MRS Code of Conduct throughout the organisation. We were the first company to sign up to the requirements and self-regulation of the MRS Code. More than 350 companies have followed our lead.

ISO 9001

This is the international general company standard with a focus on continual improvement through quality management systems. In 1994, we became one of the early adopters of the ISO 9001 business standard.

ISO 27001

This is the international standard for information security, designed to ensure the selection of adequate and proportionate security controls. Ipsos MORI was the first research company in the UK to be awarded this in August 2008.

The UK General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA) 2018

Ipsos MORI is required to comply with the UK GDPR and the UK DPA. It covers the processing of personal data and the protection of privacy.

HMG Cyber Essentials

This is a government-backed scheme and a key deliverable of the UK's National Cyber Security Programme. Ipsos MORI was assessment-validated for Cyber Essentials certification in 2016. Cyber Essentials defines a set of controls which, when properly implemented, provide organisations with basic protection from the most prevalent forms of threat coming from the internet.

Fair Data

Ipsos MORI is signed up as a "Fair Data" company, agreeing to adhere to 10 core principles. The principles support and complement other standards such as ISOs, and the requirements of Data Protection legislation.

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

www.ipsos-mori.com
http://twitter.com/IpsosMORI

About Ipsos MORI Public Affairs

Ipsos MORI Public Affairs works closely with national governments, local public services and the not-for-profit sector. Its c.200 research staff focus on public service and policy issues. Each has expertise in a particular part of the public sector, ensuring we have a detailed understanding of specific sectors and policy challenges. Combined with our methods and communications expertise, this helps ensure that our research makes a difference for decision makers and communities.

Ipsos MORI