Analysis of the full costs of cyber security breaches

Case study mini reports annex

Harry Heyburn, Andrew Whitehead, Leonardo Zanobetti
and Jayesh Navin Shah, Ipsos MORI
Professor Steven Furnell, University of Plymouth

Ipsos MORI

Contents

Introduction

This annex to the main report includes the 15 case studies as mini reports. Each case study is written up in a consistent format highlighting the nature of the cyber security breach discussed, the original and revised cost estimates, the challenges participants faced using the cost tool, and their recommendations and feedback for further development of the tool.

Case study 1

Background	
Type of organisation	Charity
Organisation size	Large (250 or more staff)
Organisation sector	Religious activities
The nature of the cyber breach	
Details of cyber breach experienced	The charity received spoof emails claiming that a hacking attack had been committed and threatening to release non-consensual recordings of staff unless they made a payment to the attackers. The series of emails was discussed in the case study interview as a single incident, and the cost reflects the total cost for the whole incident.
Length of the breach	The emails have been received for roughly the last six months and this is ongoing.
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£0
Costs identified in previous estimate	N/A
New cost estimate using the cost tool	£8,130
List of the cost categories identified using the cost tool	▪ Staff prevented from carrying out their day-to-day work ▪ Staff time spent investigating the source of the breach ▪ Staff time spent dealing with complaints from those impacted ▪ Cyber security improvements ▪ Staff time spent changing IT or cyber security policies, technical controls, processes or providers ▪ Staff training
Methodology for estimating costs	
Role of the main tool respondent	IT Manager
Other staff members involved in providing the estimate	None
Challenges in providing the estimates	The participant felt it was difficult to estimate the cost of staff time for two reasons. Firstly, they felt the staff dealing with the breach did so as part of their normal contracted activities, so did not feel this was a cost to the business. Secondly, the amount of time spent dealing with the breach was not recorded. They also found attribution of staff training difficult, as they felt this might have been brought in later regardless of this particular breach.

Costs that were not possible to estimate	They did not estimate the cost associated with shutting down their email server.
Costs that were not included in the tool	The participant felt that they couldn't record costs relating to the emotional harm to employees. It is worth noting that, in this case, this cost was borne by the individual and not the organisation, i.e. it did not necessarily result in staff taking sick leave. The nature of the incident (in terms of non-consensual video recordings of staff being made public) may have affected staff productivity, however.
Level of uncertainty attached to the estimate	There is a high level of uncertainty related to the time costs, mainly because there was a lack of understanding of the opportunity cost of time and because the time spent dealing with the breach had not been formally logged. However, costs related to new cyber security protection, which represent the majority of cost estimate, were based on receipts, so were considered to be accurate.
Comment on overall accuracy of the cost estimate	Overall, the participant felt there was a low level of accuracy with their new cost estimate. Staff time was given as an overall figure and not broken down by each granulated are of staff time costs in the tool. Furthermore, this was based on an estimate over a long period of time (six months) and thus is subject to recall error. In addition, the costs of closing down the email server were not included, potentially leading to underestimation of the full costs. However, without knowing more accurately the extent of time spent on the breach, it is not possible to know whether the estimate represents an over- or underestimate.
Feedback on the tool	
Experience in using the tool	▪ The participant felt that a lot of the material was irrelevant for their specific breach. ▪ Furthermore, they noted that it takes a long time to ensure that everything is included.
Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	None
How the tool could potentially be used by the organisation	▪ The tool could be used to show the charity's trustees the full cost of a cyber breach. ▪ It could also be used to make employees more aware of the risks related to bad cyber security practices. ▪ This could provide an estimate to provide to support an insurance claim. ▪ It could also be used to help with a risk audit.

Behaviour change as a result of a better estimate of the cost of a cyber breach	No specific changes were undertaken, although the participant highlighted the potential to change staff vigilance by showing them the impacts of a cyber breach.
Future iterations	
Ways the tool could be improved to increase its usefulness	▪ Create a bespoke tool for different types of breach. ▪ It would be more useful as an online form.

Case study 2

Background	
Type of organisation	Private sector
Organisation size	Large (250 or more staff)
Organisation sector	Administration (L) and real estate (N)
The nature of the cyber breach	
Details of cyber breach experienced	A company director received an email asking them to confirm their login details and directing them to a page that resembled their own website. When they entered their details, they began to receive undelivered messages in their inbox. A malware programme had picked up addresses from the director's contacts, taken the domain name and tried to guess other email addresses from these domain names. It sent out c.15,000 fraudulent emails stating that the company had changed its bank account details. The IT team was notified immediately but it took a few days to fully realise the effect of the breach and find all the customers that were affected.
Length of the breach	The breach was detected on a Friday and all customers were notified by the following Monday.
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£864
Costs identified in previous estimate	Direct costs
New cost estimate using the cost tool	£1861.50
List of the cost categories identified using the cost tool	▪ Staff prevented from carrying out their day-to-day work ▪ Staff time spent notifying the authorities ▪ Staff time spent notifying affected stakeholders ▪ Staff time spent investigating the source of the breach ▪ Hiring external consultants
Methodology for estimating costs	
Role of the main tool participant	Financial Controller
Other staff members involved in providing the estimate	IT Manager
Challenges in providing the estimates	None
Costs that were not possible to estimate	None
Costs that were not included in the tool	None

Level of uncertainty attached to the estimate	The participant said they had a high level of certainty with their cost. This was because accurate staff time costs were available from payroll and external costs for hiring consultants were available from invoices.
Comment on overall accuracy of the cost estimate	They assumed that there was no reputational damage, as customers were notified quickly. If this assumption is not accurate and there was some customer attrition in the long run, then the cost would be an underestimate.
Feedback on the tool	
Experience in using the tool	▪ They felt the language was suitable and easy to understand. ▪ However, navigation of the tool was difficult and involved a lot of scrolling up and down. The format seemed to be designed to be completed on paper as opposed to on a computer, which they felt would be easier.
Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	None
How the tool could potentially be used by the organisation	▪ It could be used by IT Managers to provide a business case for greater levels of cyber security. ▪ It could be used to demonstrate the cost of cyber breaches to investors, in cases where business performance is below expectations. ▪ It could be used to provide data to government, to help inform government spending decisions.
Behaviour change as a result of a better estimate of the cost of a cyber breach	The tool could inform organisations about the cost of particular cyber breaches or the potential cost of having this type of breach in the future.
Future iterations	
Ways the tool could be improved to increase its usefulness	▪ It should be designed to be computer readable. ▪ It should provide a summary sheet after completion, with the total cost and a breakdown showing the constituent costs feeding into the calculation.

Case study 3

Background	
Type of organisation	Private sector
Organisation size	Micro (under 10 staff)
Organisation sector	Finance and insurance (K)
The nature of the cyber breach	
Details of cyber breach experienced	One of the pages on the company website where the public accessed their research was taken down. The issue was quickly resolved after being spotted. In addition, their email server was blacklisted by major email providers, which meant that their emails were quarantined or sent to spam folders. This in turn meant that clients could not receive the material produced by the business. The main cost was in lost communication with their clients. Eventually the organisation was forced to change their email server. The company suspected that one of their former clients, whom they had previously given a negative report rating, was responsible for the breach.
Length of the breach	The business was unaware of when exactly it was taken down, but they estimated that it was down for around a few days. They felt the effects of changing the email server were likely to last much longer.
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£15,000
Costs identified in previous estimate	Long-term effects of the cyber breach
New cost estimate using the cost tool	The business gave a range as they initially said they didn't know some of the staff time costs. The maximum figure is therefore more comprehensive but potentially less accurate in terms of accounting for staff time: Minimum: £8,600 Maximum: £16,600

List of the cost categories identified using the cost tool	▪ Interruption of normal services provided ▪ Data or software lost, corrupted or encrypted ▪ Staff time spent notifying affected stakeholders ▪ Staff working overtime to resolve the breach ▪ Staff time spent investigating the source of the breach ▪ Changed any internal IT or cyber security policies, technical controls, processes or providers ▪ Staff time spent changing IT or cyber security policies, technical controls, processes or providers ▪ Hiring external consultants ▪ Loss of customers as a result of the breach
Methodology for estimating costs	
Role of the main tool participant	Head of Research
Other staff members involved in providing the estimate	None
Challenges in providing the estimates	The opportunity cost staff time was difficult to calculate, as the impact of the breach occurred over such a long time.
Costs that were not possible to estimate	The cost of lost customers was not possible to estimate due to uncertainty over how many customers were lost.
Costs that were not included in the tool	None
Level of uncertainty attached to the estimate	There were high levels of uncertainty in estimating the total amount of staff time involved.
Comment on overall accuracy of the cost estimate	The cost estimate provided is an estimate of the cost of resolving the issue, the majority of which reflects staff costs and the cost of external consultants. It does not include the cost of lost customers. As a result, the estimated provided is likely to be an underestimate. Even with this omission, the participant felt that their estimate of staff time was probably too low relative to the actual time spent on the breach.
Feedback on the tool	
Experience in using the tool	▪ They felt that the tool was set up to be printed out which is an out-of-date approach. ▪ However, the language was clear. ▪ It was easy to skip over the parts that were not relevant.
Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	None

How the tool could potentially be used by the organisation	The tool has illuminated the full extent of the cost of the cyber breach. Something like this would help their organisation focus on taking the appropriate action. For instance, the cost of changing the email system was relatively low and could potentially have been undertaken sooner if the full cost of inaction had been appreciated. The business would see this as increasingly useful if they grew further and employed more people to handle cyber security. Currently the participant is solely responsible for cyber security and said it is too much of a burden for them to complete alone. They would also typically not value their own time in the cost of a breach. The tool could be used both internally within the organisation and shared with the government. For instance, the granular data would have more internal use while the total figure could be shared with government.
Behaviour change as a result of a better estimate of the cost of a cyber breach	The tool could justify faster countermeasures in the case of future breaches. In this case, these measures had already been undertaken by the time of the interview.
Future iterations	
Ways the tool could be improved to increase its usefulness	▪ They felt it needs to be made into an online tool. ▪ The formatting of the comment boxes is important, as they allow people to give more context and explain their answers. This is important and the boxes should be bigger.

Case study 4

Background	
Type of organisation	Private sector
Organisation size	Medium (50 to 249 staff)
Organisation sector	Information and communication (J)
The nature of the cyber breach	
Details of cyber breach experienced	This was considered a relatively simplistic breach, involving financial theft following a fraudulent email.
Length of the breach	Less than a day
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£5,000
Costs identified in previous estimate	Direct costs
New cost estimate using the cost tool	£16,161.78
List of the cost categories identified using the cost tool	▪ Money or other financial assets stolen ▪ Change of internal IT or cyber security policies, technical controls, processes or providers
Methodology for estimating costs	
Role of the main tool participant	Managing Director
Other staff members involved in providing the estimate	Finance Manager
Challenges in providing the estimates	None
Costs that were not possible to estimate	There is a possible reputational cost with suppliers. However, it was not possible to know the extent of this.
Costs that were not included in the tool	None
Level of uncertainty attached to the estimate	Aside from the omitted cost of possible supplier attrition, the participant was highly certain of their figures.
Comment on overall accuracy of the cost estimate	High
Feedback on the tool	
Experience in using the tool	The language was clear. However, they felt the document could have been made easier to navigate.

Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	There is an informal mechanism, with the Managing Director reporting to the board on risks and the cost of those risks.
How the tool could potentially be used by the organisation	The tool could potentially be used alongside an insurance claim or police report to obtain a broader picture of the costs. The participant could see it being administered alongside other tools carried out by the Office for National Statistics.
Behaviour change as a result of a better estimate of the cost of a cyber breach	In their view, being more aware of the costs of cyber breaches increases the level of focus and awareness of those breaches. In general, attention is only given to cyber security issues when it can be shown that there is a significant financial cost attached. This would motivate people in the business to behave in a more cyber secure way.
Future iterations	
Ways the tool could be improved to increase its usefulness	It could be linked to existing government advice pages on cyber security, to help prevent similar breaches in the future.

Case study 5

Background	
Type of organisation	Private sector
Organisation size	Small (10 to 49 staff)
Organisation sector	Food and hospitality (I)
The nature of the cyber breach	
Details of cyber breach experienced	This was considered a relatively simplistic breach, where a fraudulent invoice was paid.
Length of the breach	Less than a day
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£1,900
Costs identified in previous estimate	Direct costs
New cost estimate using the cost tool	£1,900
List of the cost categories identified using the cost tool	Money or other financial assets stolen
Methodology for estimating costs	
Role of the main tool participant	Business Manager
Other staff members involved in providing the estimate	None
Challenges in providing the estimates	None
Costs that were not possible to estimate	None
Costs that were not included in the tool	None
Level of uncertainty attached to the estimate	All of the recorded cost was based on a single invoice, which was the total direct cost.
Comment on overall accuracy of the cost estimate	The participant did not include the cost of the five hours of time that they spent notifying the financial fraud team and the police, which meant they underestimated the cost.
Feedback on the tool	
Experience in using the tool	▪ In their view, the majority of the questionnaire was not relevant to their breach. ▪ However, the language was clear.

Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	None
How the tool could potentially be used by the organisation	No thoughts
Behaviour change as a result of a better estimate of the cost of a cyber breach	None
Future iterations	
Ways the tool could be improved to increase its usefulness	No thoughts

Case study 6

Background	
Type of organisation	Private sector
Organisation size	Micro (under 10 staff)
Organisation sector	Food and hospitality (I)
The nature of the cyber breach	
Details of cyber breach experienced	A staff member received a phishing email containing a fraudulent invoice. Because the nature of the invoice was similar to actual work that was being done, they initially initiated the payment. This was until the final step, at which point they checked with the original company and discovered that the invoice was fraudulent. The payment was ultimately not made.
Length of the breach	Assumed to be no time at all
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£1
Costs identified in previous estimate	None (the cost estimate was negligible)
New cost estimate using the cost tool	£20
List of the cost categories identified using the cost tool	▪ Staff prevented from carrying out their day-to-day work ▪ Change of internal IT or cyber security policies, technical controls, processes or providers ▪ Staff training
Methodology for estimating costs	
Role of the main tool participant	Owner
Other staff members involved in providing the estimate	None
Challenges in providing the estimates	All costs were related to staff time. Staff were paid hourly, so these costs were easy to estimate using the methodology presented in the tool. Likewise, if insurance or consultancy costs had been incurred these would be easily estimated using the associated invoices. However, the interviewer noted that the participant had not included the cost of their own time dealing with the incident. As an owner and not a member of staff paid hourly, the opportunity cost may be more complicated to calculate.
Costs that were not possible to estimate	None

Costs that were not included in the tool	None
Level of uncertainty attached to the estimate	None
Comment on overall accuracy of the cost estimate	The revised cost estimate, although higher than the estimate initially provided in the CSBS 2020 tool remains an underestimate as the participant did not include their own time spent responding to the breach.
Feedback on the tool	
Experience in using the tool	▪ The purpose of the tool was clear, and it was clear who was required to complete each section ▪ The tool was very long though the participant noted that this is required to be comprehensive ▪ The questions and language used were clear ▪ The Word format was not felt to be appropriate for this type of tool.
Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	None
How the tool could potentially be used by the organisation	There was a sense that this tool would be more useful for larger organisations, where it could be used to demonstrate the scale of the cost to the organisation and therefore justify changes to cyber security practices. The tool could be used reactively when a breach is experienced and might be used by high-level management to report to shareholders.
Behaviour change as a result of a better estimate of the cost of a cyber breach	None
Future iterations	
Ways the tool could be improved to increase its usefulness	Make the tool online based to improve the routing, as many questions are not relevant in all cases. As the tool will, in the views of the participant, be most useful for organisations with complex breaches with more intangible costs, additional guidance should be provided to make estimates more accurate. For example, providing guidance for assigning the extent of an impact which can be attributed to the cyber breach. It is possible that the person completing the tool may not have experience in making these types of estimates.

Case study 7

Background	
Type of organisation	Private sector
Organisation size	Medium (50 to 249 staff)
Organisation sector	Transport (H)
The nature of the cyber breach	
Details of cyber breach experienced	The cyber attack targeted the business's email servers. A fraudulent email was sent to some of their suppliers and customers purporting to come from the attacked business and informing them of a change in bank details.
Length of the breach	Two weeks
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£1,000 to £5,000 (cost range given when the business was recruited for a case study interview)
Costs identified in previous estimate	None
New cost estimate using the cost tool	£189
List of the cost categories identified using the cost tool	▪ Staff prevented from carrying out their day-to-day work ▪ Staff time spent notifying the authorities ▪ Staff time spent notifying affected stakeholders ▪ Staff time spent investigating the source of the breach
Methodology for estimating costs	
Role of the main tool participant	Finance Manager
Other staff members involved in providing the estimate	One other member of the Finance Team
Challenges in providing the estimates	Estimating the time spent by members of staff on dealing with a cyber incident could be particularly difficult to capture for larger organisations.
Costs that were not possible to estimate	None
Costs that were not included in the tool	None
Level of uncertainty attached to the estimate	The total staff time spent on dealing with the breach is an approximation, making this aspect of the costs more uncertain.

Comment on overall accuracy of the cost estimate	The estimates are considerably lower than the figures indicated in the CSBS 2020 tool, primarily because of the uncertainty around staff time costs. It is likely to be an underestimate. The estimates provided only included an average salary figure. This is because the participant did not wish for salary figures to be disclosed outside the organisation. Further to this, the participant was unable to quantify any postage costs related to notifying suppliers and customers.
Feedback on the tool	
Experience in using the tool	▪ The tool was deemed to be as long as necessary and clear in terms of language used. ▪ However, the participant noted how the current format of the tool was not user-friendly.
Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	None
How the tool could potentially be used by the organisation	The tool would be useful to gather information and to remind staff of the risks relating to cyber breaches. The data could be shared with the government, providing it is aggregated/anonymised.
Behaviour change as a result of a better estimate of the cost of a cyber breach	None
Future iterations	
Ways the tool could be improved to increase its usefulness	▪ They would prefer a PDF version of the document that could be saved and easily annotated. Alternatively, they suggested that the form could be transformed into an online tool with drop-down menus and clickable boxes. ▪ The participant mentioned that the Ipsos MORI recruiter's introduction to the tool, explaining its purpose and how to complete it, was also helpful. The document should stress clearly at the beginning that only relevant questions need to be answered.

Case study 8

Background	
Type of organisation	Private sector
Organisation size	Medium (50 to 249 staff)
Organisation sector	Administration (L) and real estate (N)
The nature of the cyber breach	
Details of cyber breach experienced	One of the organisation's employees was instructed to pay a supplier £18,000. The employee did not realise that they were not making the payment through the bank's official website. When making the payment, the employee was prompted to change the password of the organisation's account. A fraudulent payment was thus made.
Length of the breach	Assumed to be no time at all
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£1,000
Costs identified in previous estimate	Direct costs
New cost estimate using the cost tool	£438 (This does not take into account the fraudulent £18,000 payment, as it has since been recovered.)
List of the cost categories identified using the cost tool	▪ Staff prevented from carrying out their day-to-day work ▪ Staff time spent notifying the authorities ▪ Change of internal IT or cyber security policies, technical controls, processes or providers
Methodology for estimating costs	
Role of the main tool participant	Director
Other staff members involved in providing the estimate	None
Challenges in providing the estimates	▪ Assigning an opportunity cost for staff dealing with the breach proved difficult. ▪ The interviewer also noted that the participant had omitted the cost for new IT equipment that their organisation purchased as a result of the incident.
Costs that were not possible to estimate	None
Costs that were not included in the tool	None
Level of uncertainty attached to the estimate	The estimates given were felt to have a high level of accuracy.

Comment on overall accuracy of the cost estimate	The revised cost figures are lower than the estimate initially provided in CSBS 2020. The overall cost, however, is likely to be higher, as the participant failed to indicate the cost incurred for a new laptop (around £1,000, according to them).
Feedback on the tool	
Experience in using the tool	Although the contents of the tool were straightforward, the participant indicated that the length of the tool was excessive.
Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	None
How the tool could potentially be used by the organisation	The tool could be a useful instrument to assess the impact of a cyber incident – depending on the size of the breach. Larger breaches would make it more of a burden to complete the tool.
Behaviour change as a result of a better estimate of the cost of a cyber breach	None
Future iterations	
Ways the tool could be improved to increase its usefulness	▪ A final version of this tool should have automatic routing, and either work as a PDF or as an online form. ▪ Additional information on cyber breaches and how to deal with these incidents should be added to the tool.

Case study 9

Background	
Type of organisation	Charity
Organisation size	Large (250 or more staff)
Organisation sector	Education
The nature of the cyber breach	
Details of cyber breach experienced	After an academic conference, the charity's events team received an invoice from an email address that contained the name of one of the speakers and was registered with a popular email service provider. As it was felt that the £9,000 invoice had to be paid quickly, they gave instructions to their finance team to proceed with the payment. Only after the real invoice came through did the finance team requested to check the source of the first invoice. It was then confirmed by the IT department not to be a genuine email address, as it was not present in the official email address database held by the charity.
Length of the breach	This incident occurred at one specific point in time. However, a spike in phishing emails has also been recorded after that successful phishing attempt.
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£10,000
Costs identified in previous estimate	▪ Direct costs ▪ Recovery costs ▪ Long-term costs
New cost estimate using the cost tool	£13,625
List of the cost categories identified using the cost tool	▪ Money or other financial assets stolen ▪ Staff prevented from carrying out their day-to-day work ▪ Staff training ▪ Staff time spent changing IT or cyber security policies, technical controls, processes or providers ▪ Ongoing cost of vigilance ▪ Erosion of trust among staff
Methodology for estimating costs	
Role of the main tool participant	IT Director
Other staff members involved in providing the estimate	▪ One member of finance team ▪ One member of senior management team

Challenges in providing the estimates	The participant indicated that the most difficult costs to capture were those related to the staff time spent dealing with the incident. Although they felt that the daily wage figures were accurate (as they had been checked directly with the members of staff involved in the response to the attack), there was not a log of how much time had actually been spent on the incident. As a result of the breach, internal payment processing policies were changed. The cost associated with this change in the ongoing activities of the finance team was deemed more difficult to capture.
Costs that were not possible to estimate	The participant noted, anecdotally, that the first attack seemed to have opened the way to further phishing attempts. They felt this produced an ongoing cost related to vigilance against threats.
Costs that were not included in the tool	The interviewee underlined that the incident had reduced trust among colleagues. They felt this was a genuine cost but one which would be hard to quantify and is not currently captured within the cost tool.
Level of uncertainty attached to the estimate	The participant stated that their responses were reasonably accurate, give or take around 10 per cent. Additional time to complete the questionnaire would not have improved the estimates.
Comment on overall accuracy of the cost estimate	Although the revised cost figures are higher than the estimate initially provided in the CSBS 2020, these do not include two costs that were identified by the participant in the interview and not recorded on the cost tool (the ongoing vigilance cost and trust erosion).
Feedback on the tool	
Experience in using the tool	The participant deemed the language of the tool to be clear enough. This participant was sent a previous version of the questionnaire and, later, a heavily updated version, which was shorter and more visually appealing. They believed that the second version was more suitable for its purpose because it was shorter and easier to navigate, and because it followed a more logical order. The length of the tool was believed to be justified by the different types of costs covered.
Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	None

How the tool could potentially be used by the organisation	At present, the organisation's senior management team are not interested in estimating the opportunity cost in the aftermath of a cyber security incident, because they are not keen on adding to staff workloads. The tool could be particularly useful in the future in case of a large breach, or if a particular breach continues over a long period of time.
Behaviour change as a result of a better estimate of the cost of a cyber breach	None
Future iterations	
Ways the tool could be improved to increase its usefulness	▪ The participant suggested that the tool could be more accessible in other formats (e.g. online), allowing them to filter questions based on previous answers. ▪ They suggested that the questions asked could be tailored depending on the type of breach suffered.

Case study 10

Background	
Type of organisation	Charity
Organisation size	Large (250 or more staff)
Organisation sector	Education
The nature of the cyber breach	
Details of cyber breach experienced	A member of staff from HR sent out an email to another organisation requesting a reference for a candidate. As the other organisation's email address had been hacked, a phishing email was sent in response to the reference request. The member of staff opened what looked like a DocuSign link and entered their credentials. They did not realise immediately that the fake document attached mentioned "invoice", and so did not report the incident. Sensitive personal information of staff and candidates was thus exposed. Hundreds of phishing emails were then sent out from the compromised email account.
Length of the breach	One week passed between the first unauthorised access to the servers and the moment in which the phishing emails were sent out.
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£53,000
Costs identified in previous estimate	▪ Direct costs ▪ Recovery costs
New cost estimate using the cost tool	£55,069
List of the cost categories identified using the cost tool	▪ Staff prevented from carrying out their day-to-day work ▪ Staff time spent investigating the source of the breach ▪ Hiring external consultants ▪ Staff time spent notifying the authorities ▪ Staff time spent notifying affected stakeholders ▪ Staff time spent dealing with complaints from those impacted ▪ Change of internal IT or cyber security policies, technical controls, processes or providers ▪ Provision of additional cyber security protection to customers, investors, suppliers
Methodology for estimating costs	
Role of the main tool participant	Head of IT – responsible for security, infrastructure, and strategy

Other staff members involved in providing the estimate	None for this tool, although for a previous evaluation of the cost of this breach the participant liaised with their manager, which coordinates HR, IT, and Finances.
Challenges in providing the estimates	The participant noted that some of the information required might not be public knowledge. However, the participant mentioned that some of the questions included terms which were unclear or ambiguous.
Costs that were not possible to estimate	Opportunity cost was deemed as nearly impossible to capture accurately because of the complexity. The response involved a suspension of any IT-related activity and a scan of each member of staff's laptops. Thus, staff members returned to their daily tasks gradually and at different times, meaning they would all need a bespoke entry in the current tool.
Costs that were not included in the tool	The participant had to provide cyber security insurance cover as compensation to external partners and customers affected by the breach. They felt that the tool did not have the space to record these costs (around £120 per insured individual). However, it is worth noting that the cost tool does attempt to capture insurance premiums as well as customer compensation, and this was missed by the participant.
Level of uncertainty attached to the estimate	The participant suggested there was probably a 10 per cent margin of uncertainty, especially around opportunity cost figures which were broad estimates.
Comment on overall accuracy of the cost estimate	Although the revised cost figures are higher than the estimate initially provided in the CSBS 2020, they still exclude other costs mentioned by the participant during the interview, such as the insurance premium compensation payment for those affected by the attack.
Feedback on the tool	
Experience in using the tool	The participant indicated that logging hours or days spent dealing with the incident and its aftermath was not straightforward and was burdensome, given the large number of employees to account for. Further to this, they felt that some questions seemed to be overlapping.

Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	After the incident, the organisation carried out their own evaluation of the cost associated with the breach. This analysis covered: ▪ Staff-related costs (estimated number of days, broken down by staff bands) ▪ Costs to other involved users ▪ Number of users affected ▪ Other costs (including cyber insurance costs and upgrade of security systems)
How the tool could potentially be used by the organisation	The participant indicated that this tool would probably not be used by the organisation. The participant highlighted that the tool seems to be too complex for operational use and that they already had their own process for cost estimation. Moreover, its length could make it excessively burdensome in a cyber breach scenario, when there are more immediate pressures to resolve the incident.
Behaviour change as a result of a better estimate of the cost of a cyber breach	Demonstrating the full entity of a cyber breach would lead staff to be more aware of threats relating to cyber breaches.
Future iterations	
Ways the tool could be improved to increase its usefulness	▪ A glossary should be introduced. ▪ Hyperlinks could help participants to quickly move onto new sections. ▪ Making boxes clickable and moving the tool online would improve the experience. ▪ Clarify whether opportunity costs refer to a single individual or bands of individuals. ▪ Adding rows rather than columns in the table would allow organisations to overcome formatting issues.

Case study 11

Background	
Type of organisation	Private sector
Organisation size	Medium (50 to 249 staff)
Organisation sector	Finance and insurance (K)
The nature of the cyber breach	
Details of cyber breach experienced	Some customers were sent other customers' one-time passcodes when using the telephone-based services provided by the organisation. This was found to be due to the system failing to handle large amounts of requests at once.
Length of the breach	A one-off occurrence
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£24,000
Costs identified in previous estimate	▪ Direct costs ▪ Recovery costs ▪ Long-term costs
New cost estimate using the cost tool	£21,515
List of the cost categories identified using the cost tool	▪ Staff time spent notifying affected stakeholders ▪ Staff time spent investigating the source of the breach
Methodology for estimating costs	
Role of the main tool participant	Data Protection Officer – also in charge of HR when incident took place
Other staff members involved in providing the estimate	6 members of staff, from: ▪ Data protection team ▪ Communications team ▪ Legal team
Challenges in providing the estimates	Estimating the time spent by members of staff dealing with a cyber incident was difficult, as the incident happened several months prior to the interview and the organisation had no log of time spent on dealing with the issue.
Costs that were not possible to estimate	Phone bills
Costs that were not included in the tool	The participant felt that the tool did not let them record costs relating to reputational damage. It is worth noting that the cost tool does attempt to capture the costs *arising from* reputational damage, such as customer attrition and that this may have been missed by the participant.

	Similarly, the participant noted that the company share price might be affected for publicly listed companies and that this was not included in the tool. As previously noted by the authors, isolating the effect of a cyber security breach on a company's stock price presents systematic challenges beyond the scope of this study, which is why it is omitted from the cost tool. However, there may be a need to explain inclusions and omissions to users in the tool guidance.
Level of uncertainty attached to the estimate	The participant indicated that IT costs related to solving the incident are accurate, as they referred to the total budget for that specific task, including staff costs. These represented around 90 per cent of the total costs incurred. Other costs, such as opportunity cost of investigating the source of the breach or contacting stakeholders, were deemed less accurate.
Comment on overall accuracy of the cost estimate	The revised estimates are lower than original estimates. However, this may be because any costs associated with reputational damage and loss of shareholder value were not included (but may have been included, even if broad and uncertain, in the CSBS 2020 estimate).
Feedback on the tool	
Experience in using the tool	The tool was deemed to be as long as necessary if it was intended to gain an in-depth picture of the costs, and clear in terms of the language used.
Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	None
How the tool could potentially be used by the organisation	The participant mentioned that the tool would be useful in case of a larger breach. The tool could also be used to identify good practices and make a business case around data protection issues. The data could be shared with the government providing it is aggregated/anonymised.
Behaviour change as a result of a better estimate of the cost of a cyber breach	None
Future iterations	
Ways the tool could be improved to increase its usefulness	The participant recommended a PDF version of the document that contained clickable boxes.

Case study 12

Background	
Type of organisation	Private sector
Organisation size	Medium (50 to 249 staff)
Organisation sector	Utilities (BDE) and manufacturing (C)
The nature of the cyber breach	
Details of cyber breach experienced	A fraudulent email was sent out to an HR director requesting a change to an employee's bank account details. The changes were made, and the employee's salary was paid into the fake account.
Length of the breach	0
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£5,000
Costs identified in previous estimate	▪ Direct costs ▪ Recovery costs
New cost estimate using the cost tool	£2,892
List of the cost categories identified using the cost tool	▪ Money or other financial assets stolen ▪ Staff time spent investigating the source of the breach ▪ Staff time spent changing IT or cyber security policies, technical controls, processes or providers
Methodology for estimating costs	
Role of the main tool participant	IT Manager
Other staff members involved in providing the estimate	The participant completed the tool on their own, but their responses build on a previous internal analysis, for which information was collected from: ▪ HR staff ▪ Finance staff
Challenges in providing the estimates	None
Costs that were not possible to estimate	None
Costs that were not included in the tool	The participant felt that they couldn't record costs relating to reputational damage, leading to a loss of customers. It is again (as per the previous case study) worth noting that the cost tool does attempt to capture customer attrition and that this might have been missed.
Level of uncertainty attached to the estimate	The participant was confident of their estimates, as they had been sourced from their earlier internal report.

Comment on overall accuracy of the cost estimate	As noted above, the participant was confident about the estimates given. However, the interviewer noted that they had omitted the time cost of a fourth member of staff in deploying improved cyber security measures. The original CSBS cost estimate included additional costs from other, similar fraud attempts that were unsuccessful. Therefore, even though the revised cost estimate is lower, it might still be considered a more accurate representation of this specific breach.
Feedback on the tool	
Experience in using the tool	▪ The purpose of the tool was clear. ▪ The language was clear, although the notion of a "breach" initially signalled to this business that the tool was for costs associated with successful cyber attacks. They noted that unsuccessful attacks (which the tool can also be used for) could also incur significant costs in terms of investigation and new measures being put in place. ▪ The questions were considered appropriate but, at times, narrow in their response options. ▪ The tool is lengthy and parts of it could be condensed.
Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	The business already uses logs of staff time dealing with the breach and salary figures to estimate time costs. In addition, they have previously attempted to include reputational costs and ongoing training costs.
How the tool could potentially be used by the organisation	In their view, this tool could be effectively used to capture the cost of a successful breach attempt. Data could be shared with the government providing it is anonymised.
Behaviour change as a result of a better estimate of the cost of a cyber breach	None
Future iterations	
Ways the tool could be improved to increase its usefulness	▪ An interactive PDF would be more user-friendly. ▪ Exact salary amounts might be too sensitive to disclose in a tool like this, so salary bands should be clearly specified.

Case study 13

Background	
Type of organisation	Private sector
Organisation size	Large (250 or more staff)
Organisation sector	Administration (L) and real estate (N)
The nature of the cyber breach	
Description of the nature of the cyber breach	Someone in the business downloaded a malicious file, which put ransomware on the network. No one could connect to the network once the ransomware was active.
Length of the breach	The malicious file was introduced on Saturday, started to cause disruption on Monday night and was detected at 6am on Tuesday morning. It took four days before servers were back to normal for everyone.
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£200,000
Costs identified in previous estimate	None
New cost estimate using the cost tool	£300,000
List of the cost categories identified using the cost tool	▪ Staff prevented from carrying out their day-to-day work ▪ Data or software lost, corrupted or encrypted ▪ Damage to IT equipment
Methodology for estimating costs	
Role of the main tool participant	Director of IT
Other staff members involved in providing the estimate	None
Challenges in providing the estimates	None
Costs that were not possible to estimate	The participant had to inform clients of the breach, which may have had a reputational effect. However, while they had considered this when running through the cost tool, they noted that there was, for the moment, a lack of concern on the part of their clients.
Costs that were not included in the tool	None
Level of uncertainty attached to the estimate	Wherever wage rates were used in the cost calculations, these were best guesses of other employees' wage rates, which makes these costs less certain.

Comment on overall accuracy of the cost estimate	The participant thought the cost tool offered a compressive structure for estimating costs. For them, it ensured that businesses would not ignore the indirect time costs that may have otherwise been overlooked.
Feedback on the tool	
Experience in using the tool	▪ They are a long-term employee with an understanding of all the financial aspects of the business. A less experienced IT director or someone new to the business would require more assistance from the Financial Director when completing a tool like this. ▪ The purpose of the tool was clear. ▪ The language was clear, with no ambiguities. ▪ The questions were appropriate and comprehensive.
Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	None
How the tool could potentially be used by the organisation	The participant suggested that the tool could help validate IT Managers' cost estimates when they raise them with senior staff in an organisation. This could help build the business case for further investment in cyber security.
Behaviour change as a result of a better estimate of the cost of a cyber breach	The following changes were put in place after the breach, so further changes based on using this tool were not considered as necessary: ▪ Moving from Windows 7 to Windows 10 ▪ Passwords being reset more frequently, and the same passwords not being used across systems ▪ The VPN service now has two-factor authentication ▪ They are working towards ISO certification
Future iterations	
Ways the tool could be improved to increase its usefulness	▪ An online tool, with the option to access a condensed version of the full tool would be helpful. ▪ It should allow organisations to cost up hypothetical breach scenarios to help them plan ahead.

Case study 14

Background	
Type of organisation	Private sector
Organisation size	Micro (under 10 staff)
Organisation sector	Health and social care (Q)
The nature of the cyber breach	
Description of the nature of the cyber breach	A fraudulent invoice of £300 for a company that did not exist was sent to the organisation's accountant. The breach was identified at this point and no payment was processed.
Length of the breach	Assumed to be no time at all
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£0
Costs identified in previous estimate	None
New cost estimate using the cost tool	£600
List of the cost categories identified using the cost tool	▪ Staff time spent investigating the source of the breach ▪ Staff time spent changing IT or cyber security policies, technical controls, processes or providers
Methodology for estimating costs	
Role of the main tool participant	Managing Director
Other staff members involved in providing the estimate	None
Challenges in providing the estimates	None
Costs that were not possible to estimate	None
Costs that were not included in the tool	None
Level of uncertainty attached to the estimate	No major thoughts offered – the participant was relatively happy about their estimate
Comment on overall accuracy of the cost estimate	As above, no major thoughts offered
Feedback on the tool	
Experience in using the tool	▪ The purpose of the tool was clear. ▪ The language was clear, with no ambiguities. ▪ The questions were appropriate and comprehensive.

Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	None
How the tool could potentially be used by the organisation	The tool could be used to review internal cyber security practices and validate actions taken after a breach.
Behaviour change as a result of a better estimate of the cost of a cyber breach	The tool helped the participant to think about a wider range of costs beyond the direct costs of the breach. As the invoice was not paid, the participant originally assumed the breach incurred no cost. However, after completing the tool they realised they had not accounted for the time cost of dealing with the breach (e.g. preparing internal comms and reconfiguring email spam filters) or the time cost for providing increased cyber security protection (e.g. researching remote anti-virus software and admin time to updating software). It has also, in the participant's mind, validated the actions they took following the breach, in terms of getting more advanced anti-virus software, new training material and taking more precautions when processing invoices.
Future iterations	
Ways the tool could be improved to increase its usefulness	The main suggestion was to bring the tool online, with the functionality to triage users to the appropriate sections.

Case study 15

Background	
Type of organisation	Private sector
Organisation size	Medium (50 to 249 staff)
Organisation sector	Administration (L) and real estate (N)
The nature of the cyber breach	
Description of the nature of the cyber breach	An employee received a phishing email, which posed as a Microsoft admin email. The individual entered their login details, at which point the attacker was able to gain access to their email account and send out the same phishing email to all of their individuals contacts.
Length of the breach	One day to initially identify and resolve the breach, with remote email access down for a further two days.
Estimated cost of the breach	
Previous cost estimate (CSBS 2020)	£1,500
Costs identified in previous estimate	None
New cost estimate using the cost tool	£1,800
List of the cost categories identified using the cost tool	▪ Staff time spent investigating the source of the breach ▪ Staff time spent changing IT or cyber security policies, technical controls, processes or providers ▪ Data or software lost, corrupted or encrypted
Methodology for estimating costs	
Role of the main tool participant	Head of IT
Other staff members involved in providing the estimate	None
Challenges in providing the estimates	The most challenging part was estimating salaries and time lost per individual staff member.
Costs that were not possible to estimate	No cost was estimated for the potential reputational damage caused from emails going out to external clients. The business had contacted all 400 of the clients on their contact list and clients had not raised concerns about it.
Costs that were not included in the tool	None
Level of uncertainty attached to the estimate	No major thoughts offered – the participant was relatively happy about their estimate, although there was greater uncertainty associated with the time costs due to having to estimate salaries and time lost for each staff member.

Comment on overall accuracy of the cost estimate	The participant noted that, while difficult, they tried to be as accurate as possible in calculating the cost of staff time.
Feedback on the tool	
Experience in using the tool	▪ The purpose of the tool was clear ▪ The language was clear, with no ambiguities ▪ The questions were appropriate and comprehensive ▪ Usability was an issue – the participant found it very repetitive when trying to calculate the cost of staff time for multiple staff. They particularly wanted this aspect to be condensed in any future tool.
Behaviour change	
Method currently used by the organisation to estimate the cost of a cyber breach	None
How the tool could potentially be used by the organisation	It could potentially provide organisation with more robust evidence to justify greater investment in cyber security and training for employees.
Behaviour change as a result of a better estimate of the cost of a cyber breach	No major thoughts offered
Future iterations	
Ways the tool could be improved to increase its usefulness	▪ Similar to other participants, it was suggested here that an online tool, with the option to access a condensed version of the full tool would be helpful.

Ipsos MORI's 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.

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.

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.

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.

Data Protection Act 2018

Ipsos MORI is required to comply with the Data Protection Act 2018. It covers the processing of personal data and the protection of privacy.

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