GOWLING WLG

HOW TO DEAL WITH A DATA SECURITY BREACH

24 June 2015

This podcast looks at cyber security, paying particular attention of how to deal with a data security breach.

With organisations holding considerable amounts of sensitive data they are continuing to be targeted and at threat from having such data compromised or hacked. Most organisations have in place procedures and processes in place in an attempt to reduce the risk that sensitive data is exposed to. However, even those with robust cyber security can be compromised.

As such all organisations need to be prepared and aware of what their immediate response should be once they discover that their sensitive data has been compromised or hacked.

In this podcast Partner, Patrick Arben, and Helen Davenport, a Director in our Tech team offer organisations their recommendations, including three key "top tips" for what organisations should do before, during and after a suspected data breach.

Your browser does not support the audio element.

Subscribe

Transcript

Presenter: Hello, I'm joined by Director, Helen Davenport, and Partner, Patrick Arben, both members of Wragge Lawrence Graham & Co's Tech team. Today we're going to be looking at Cyber Security and how to deal with a data security breach. So Patrick, what should an organisation's immediate response be as soon as it becomes aware that its

sensitive data has been compromised or hacked?

Patrick Arben: Well clearly time is going to be of the essence and there is a need to respond rapidly and ideally an organisation should have in place long before it needs to call upon it, an incident response plan. That incident response plan really needs to identify a response team with key roles and responsibilities identified so you're going to need to nominate a lead to deal with the incident, and you're going to ensure that there is appropriate representation and stakeholder input from across your organisation so that may mean that you've got to put together a cross-disciplinary team of maybe HR people, IT people and management to address the issue and make rapid and sometimes make really quite business-critical decisions. The immediate response is going to be looking at what's happened, trying to understand what's happened and stop any further data loss and to preserve the integrity of your systems as far as you possibly can. In order to do that, you're going to need technical expertise and you may have that in-house but, if not, you're going to need to bring in external help, cyber security experts who can drop everything and come and help you at short notice. In order to achieve that, you're probably going to have to have a list of approved suppliers in place that you can call upon when you need them. On the basis that you are able to identify what the hack is and what data has been lost and you're able to put a stop to that you may then need to consider whether there are any critical decisions to be made. Do you need to immediately notify the police? If you think or suspect an internal or inside job hack involving some misconduct by employees, do you need to suspend employees? Do you need to disable any aspects of your system and escalate this up your business to try and identify and understand what the implications of that might be in terms of business continuity? Then I think you probably need to consider whether to engage external counsel for any urgent and immediate legal advice. You may well have a data protection officer in place, but that data protection officer may not be a lawyer. The advantage of retaining either an in-house lawyer or external counsel is that you would be able to claim legal professional privilege over any advice that's received. And then finally in terms of that immediate response, you may need to consider notifying insurers if you have a cyber-risks insurance policy.

Presenter: Following on from that immediate response what is the next step in the process?

Helen Davenport: Well as Patrick has said, critically you will put together an instant response team and you will be aiming, as part of the first stage, to stop any further data loss, and it may be that it's immediately apparent what has happened but very often it is not, so then the next stage will be to do a much more detailed investigation, with the help of your instant response team to try and find out what happened and why, and that

investigation will potentially involve a number of aspects. You may have already retained some external IT resource to help you with that investigation or you may be carrying the IT work in-house but you probably will need some IT expertise for the purposes of the investigation. Invariably there will be a degree of data review whether that might be access logs or it might be email records, particularly if an employee may be suspected, and very often in such investigations we get involved in interviewing key employees. There is also the possibility of potentially making applications to Court, possibly to obtain information from third parties that may enable you to get to the bottom of what's happened. As you start to learn more about what's happened you then to revisit the question of 'Is there any more you can do about stopping further data loss?' and making sure that you preserve any further data that you can. As part of that investigation, it is also very important to bear in mind whether personal data may have been impacted because consequences follow from that. You will need to consider who is the data controller and who is the data processor and the respective responsibilities. You will also be looking at whether this is a serious breach. The reason for that is whether that will cause you to have to actually notify the information commissioner. As the law stands at the moment, there is no automatic obligation to notify but the ICO's office expect that serious breaches, and that's measured by the volume of records impacted and the sensitivity of the data; that those serious breaches would be notified. You might also need to consider notifying the data subjects themselves. In carrying out the investigation a final point to bear in mind is to make sure that you don't actually end up committing an offence yourself by tripping yourself up, and therefore to be aware of potential offences that could be committed under the Data Protection Act, Computer Misuse Act or the Regulation of Investigatory Powers and Lawful Business Practice Regulations. Depending on the nature of the data, and also the jurisdictions impacted. You might also need to bear in mind the laws of other countries to make sure that what you're doing isn't going to cause you an issue down the line.

Patrick: Just building on the points Helen made, there may also be others who you will need to notify, other stakeholders who will need to be notified as well as the information commissioner. Say for example, if you are a regulated industry, you may need to notify your regulator, you may need to notify other stakeholders, so there may be data processors who you are contracting with who are affected by this, or you may need to consider notifying individuals whose personal data has been compromised, and there's a judgement call to be made there as to whether that would be an appropriate response in circumstances where you don't necessarily know the extent to which that data has been compromised. You're going to need to think about rebuilding compromised IT systems and there is going to be a time and cost associated with that and you're going to need to think

about reputational issues and to the extent that this becomes a public hack and it may be that this comes into the public domain through other sources. Its important to have press statements and communications/scripts, ready to go on a reactive basis if you are faced with some adverse and unexpected publicity and there are cyber risk insurance policies that will offer that service in addition to legal assistance and technical assistance. You may need also to consider whether it's appropriate to pursue the perpetrators of the breach or the hack because you may well have suffered loss and that loss could come in a number of different guises and you may need to recover physical assets or data from whoever has perpetrated the hack. So there could be disciplinary issues if this has been a hack perpetrated by an employee, for example a disgruntled employee. Alternatively you may want to pursue civil claims for compensation and remedies through the courts, for example you may have a claim against an IT services provider who for example has through some act or omission on their part allowed your systems to be compromised or you may have claims against a third party data processor an outsource service provider who has allowed your data to be compromised or misused. So there may be contractual claims that you can bring for compensation. Finally, you are also going to need to consider whether it is appropriate to involve the police if you feel that there have been criminal acts perpetrated. In terms of involving the police, obviously the more comprehensive and thorough investigation you have done, if you can present that information to the police at the outset you're going to make their life easier and you're going to hopefully enthuse and encourage them to investigate that crime on your behalf.

Presenter: So once an organisation has concluded its investigations, what should it be doing next?

Helen: We've talked about the stages of addressing a data security breach so the immediate response, the investigation, then the steps that you might take to remediate or address the particular incident, it's then really important to evaluate everything that's just happened and consider how successful was the response? You might need to consider whether actually your incident response plan, if you had one in place, how might it be improved to enable you to respond better next time or indeed, if you didn't have one, to put one in place. There may be work that needs to be done to educate individuals within the organisation about the risks of breaches as there may be steps that they can take to prevent such issues or at least try and prevent issues occurring in the future. In tandem within this, potentially updating policies and procedures within your organisation, and again that lies with sort of education and training but there may also be technological things that you can do to improve your security.

Presenter: OK, so finally what are your top tips for dealing with a cyber-security breach?

Helen: I think there are three top tips really to bear in mind. The first one, be prepared and act quickly but in acting quickly don't forget about key issues such as insurance; deploy your instant response plan that hopefully you will have already put in place.

Patrick: And just building on Helen's point around the incident response plan, that plan is going to be easier to implement if you've had some essentially dry runs first, so you've tested that plan beforehand and worked out where the wrinkles and where the issues might be and refined it, so I would certainly say rehearse that plan on a regular basis if possible.

Helen: Our second tip is to really make sure you manage the investigation into the incident, keep control of it and to share information exclusively on a need to know basis because you don't know at the outset exactly how the breach may have occurred and you don't want to potentially tip off or even create a further incident when people understand what's happened and in managing the investigation, try and ensure that you keep documents privileged if at all possible by involving a lawyer, and finally make sure that the investigation is fully documented because it may be that down the line you need to justify particular decisions that you've taken and a really good audit trail will really enable you to do that. Our third tip, make sure you then have a strategy once you've investigated the incident. As the law stands at the moment you don't automatically need to notify the Information Commissioner's Office, but you will need to think about the pros and cons of doing so. You will also need to think about the pros and cons of notifying others, data controllers, processors, subjects, regulators and others, and how is that going to fit in with your PR response if you need to have one. So in summary I think it really is, be prepared and act quickly, manage the investigation and have a strategy so that your response to the incident is controlled and decisions you want to take aren't overtaken by events.

Presenter: Thank you both and thank you for listening. I hope that you found that interesting and useful. If you have any further questions please don't hesitate to get in contact with anyone from the Tech team here at Wragge Lawrence Graham & Co. Thank you.

Related Tech, Digital Risk

Host(s)

Patrick Arben

Partner - Birmingham

Email

patrick.arben@gowlingwlg.com

Phone

+44 (0)121 393 0011

vCard

Patrick Arben

Helen Davenport

Partner - Birmingham

Email

helen.davenport@gowlingwlg.com

Phone

+44 (0)121 393 0174

vCard

Helen Davenport