satswana

Company registered number 09329065 www.satswana.com

Satswana Cyber Protection

We received a very sensible request for support from one of our customers regarding a Cyber Security threat, and decided that the result should be shared with all our customers

1 Protection better than cure

Clearly effective protection is always going to be better than a cure, so our first concentration must be on that aspect, there are three key planning points

1. Encrypt your data at rest. That keeps it safe even if you are hacked, but it is not a protection against ransomware. We prefer you to use encryption for sensitive data in transit
2. Take an offline backup of your data and keep it in a place that is not attached to a network. Do it as often as you think necessary, but once a month would mean that in the event of a ransomware attack you have a "history" file to go back to, even if you have lost a month of current data. If you do lose a month (or two) that will be tough to rebuild, but it is possible, since other people will have had the counterpart to information (on emails for instance) that you have shared, and once your system is clean again – then you can ask them to give you the correspondence back. What you cannot be expected to do is to rebuild your history from scratch – which is where the offline backup comes in. (Please note our comment on ransomware below; online backups are almost certainly useless.)
3. The third point is going to be the one that gives us the most work, and that is to analyse what we are doing in the first place. For this purpose we insert a systems analysis spreadsheet, more also on that below

2 Know your system

Almost every school is going to have a different starting point. Some may still have a heavy reliance upon "paper" based files and spreadsheets – and we would contend that there is nothing wrong with that, providing files are securely locked. The raw fact is that a criminal cannot encrypt a paper file and it can provide the optimum backup! Others will have an "on premise" server, and once again there are huge advantages of maintaining the data on your own property – not least because you will not have to rely on a broadband network. It may interest readers that the latest thinking from IBM embraces a "hybrid" approach, despite a huge concentration on their business being to provide "cloud" data, because you can maintain a local cache that speeds responses. It is not always Luddite to be behind the curve!!

That is not to criticise those who may have gone for a totally Cloud solution – we are all tending that way as we adopt either Microsoft 365 or Google Cloud to provide support tools. Many will rely upon what was the original "grids for learning" approach, and that specialist filter on your data could potentially be very helpful, especially where they restrict web access to safe sites, but we contend that they need to up their game considerably, as does the whole education software provider industry. More on that below

The point is that you almost certainly will not know what you have, and if you do you may not know whether you are doing everything you should to make it work – or indeed what is required to do so.

The inserted systems analysis spreadsheet (Appendix C) is designed to be a starting point to gather the required information on where you are now. It may need modification and additions, and you may discover considerable resistance to its completion, in which case you have gained an immediately essential bit of "intelligence" from the exercise. Why oppose gathering information? There are probably two answers, the first being that "knowledge is power" – and if you do not know what I know, then I cannot be questioned. The other (very human) reason is a "resistance to change" that is especially deeply embedded in all aspects of matters IT that we must be sympathetic to, but both these negative forces just help the criminals to escape analysis. Satswana recognises that we are probably asking the entire IT support industry within education to totally relearn everything from scratch and abandon years of experience that has given them current skills. But that is what it takes, because "the enemy" is not resting on its laurels, it spends every waking moment thinking up new ways of penetrating every defence you construct. We have to preach that in matters "cyber" change is a constant.

Thus the purpose of the analysis is to give all school leaders (and Governors) an insight into where we start from? What is it costing us? Where are we delinquent? What are the options available to us? How would that affect our budget? What can we learn? Are we more secure as a consequence of the study?

3 Failure is built in

If we are to make something better, then we have to be able to be honest about the reasons why current systems are not fit for purpose

As this regards software our "Satswana Data Briefing" paper (inserted at Appendix A but available as a separate document) explains the deficiencies in that area

When it comes to the distribution infrastructure that we now call "the Internet" we have a different problem, in that the essence for many people is that this should be free, open, and devoid of regulation. The result has been unparalleled inventiveness and creativity in so many areas that have benefited society. Unfortunately however a high percentage of that brilliance has been dedicated to fraud and criminality.

Many of the support structures have "grown like Topsy", developing organically rather than being based on a plan, so actually we are all ending up fighting for updates within the very establishment that should be protecting us, who are equally resistant to change, or perhaps a fairer view might be that they are comfortable with what they know and seek to avoid the cost and disruption that an updating exercise would involve. However, we should hold them to account for a continued "soft" reliance on licensing software that has long since ceased to be fit for purpose – whereas they could have been (indeed still could be) material agents of change. To discover that one significant former local authority provider had not even applied encryption to their data at rest was intensely disturbing, and the whole issue of backup security has generally failed to embrace a protection against ransomware. Either the "grids for learning" must up their game considerably, providing cyber leadership to match the manner in which they provide web access protection, or somebody else will fill the vacuum.

The logical alternative suppliers are the people who already control all the broadband access, the Internet Service Providers, and here again we generally find a failure in ambition or intent – indeed possibly a conflict of interest. Do they calculate that just so long as customers are buying expensive services from them to manage downstream risk, then they have no incentive to control it at source?

Looking at this from a school leadership perspective, if the providers of software that you (very expensively) provide for a cosy existence fail to invest in change, matched only by an equal failure by the distribution industry in all its forms, then how are you – with your prime directive being to teach – going to change things?

Satswana contends that the answer starts with awareness that you are being under served, taken advantage of, left in the front line of being expected to protect personal data without the support tools you need, in almost every possible area we can think of. Thereafter you have the fantastic power of your cheque books, because you "pay the piper". After awareness comes organisation – whether that be from the DfE, new commercial investors who embrace the opportunity (could that be BT, or the recent purchasers of SIMS?), or a cooperative created from within the community itself. The result has to be lower costs, increased automation, less complexity and massively improved performance.

4 What are we looking for?

Put in lay terms, if you know that you get phone calls from an annoying source, you block them, right? You would never consider continuously answering them! This can be done very easily on the Internet and really it should be mainstream at all levels of provision, but sadly it may not be because of the belief that you let everything through. Any "next generation" firewall will have the capability to hold tables of known criminal sources that they can refuse to talk to – it is known as threat intelligence and there are organisations constantly assessing new threats and updating those tables every twenty minutes as the exploiting IP address moves around seeking to evade detection. Protecting the perimeter must be considered a basic defence – and this is possible with an on premise server as well as through the Cloud – together with creating a "white list" of allowed websites, meaning that students can only access what you have approved from your network.

A second essential is a backup structure that is either immune to ransomware, or that can recognise a rogue .exe file. There are many ways of achieving this, but you may well be dismayed by the answers you get when you ask the question. That is why (at the moment) taking an occasional offline copy of your history is so important.

If your perimeter is protected by all the usual methods, and you can restore your data if you are attacked, whilst denying an attacker access to the raw information because it is encrypted – and at the same time you are controlling where staff or students can go on the Internet, then you will have done a very good job.

Cyber essentials

Not that you are finished, there is so much more to the passive and active defence of a computer system than just the network and most of that comes from the access methods required by users to talk to the system (often referred to as end points). That in turn requires personal knowledge and training which may come naturally to those who have been interested in gaming or social media, but much harder to those who have escaped those pastimes. Appendix B contains two training videos for staff (originally published in our June 2021 update) – but you will gain a more comprehensive understanding from seeking to meet the Cyber Essentials requirements of the NCSC that you will find here https://www.ncsc.gov.uk/cyberessentials/overview.

Whether or not it is worth the cost and time of achieving full certification must be a matter for your executive, but in any event the "self-assessment" approach will almost certainly give you many things to think about, even if you do not adopt them all immediately. You may possibly ask yourself why these features are not built into the infrastructure in the first place, and to be fair both Microsoft, Google and the smartphone providers have come a very long way to do so, and continue to roll out protection.

Reacting to a threat

If you think that something might have happened, or you are just concerned that it is possible, then please call Satswana immediately. We have to caution that in the last six months ransomware attacks have successfully penetrated schools, and at the same time they have become much more capable and sophisticated. There is no question of paying the ransom, even if you could afford it, not least because you will probably lose your money as well as your data. Equally it is probably going to be impossible to recover the data, so knowing that you have your history secure at some point in time becomes absolutely essential. Stealing personal data is impossible if you hold it in an encrypted form, so the greatest current risk to your operation is a ransomware attack, so take that backup, please!

In conclusion

Cyber security is a very complex and troubling subject that should be being addressed much more professionally by many aspects of the Internet structure which is too wedded to a laissez faire approach. You can only do your best, but to repeat, encrypt your data at rest (and in transit if it is sensitive). Protect your history with a secure off line backup. And demand the information you need to establish where you currently stand before joining a clamour for change. Please remember that you hold the purse strings

Appendix A

Satswana Data Briefing

1 Purpose

The aim of this document is to provide a briefing for the lay individual that will explain the risks and restraints associated with managing information on a computer, especially with regards to the protection of personal information – a requirement of the Data Protection Act 2018. To start at the beginning, data is just a word meaning information – your name and address for instance – something about you that has to be stored and referenced. Once upon a time it would have been written down on a piece of paper, and there is no essential difference when you store that in a computer, except that it can be managed and manipulated by a software program to give you a range of answers. Do not, please, be bamboozled or put off by the language of computing because it has all been invented over the last 50 years or so and refers originally to something that the writer understood and sought to explain. For instance a "bug" – a word often used to describe a problem in computing – was originally a moth that became electrocuted in an early IBM machine, creating problems for both parties! What went wrong? "There was a bug in the computer"!

2 What you can do

We will go into some depth as to why, but straight away may we please say that every Trustee/Governor/Head/Leader in Education/IT expert – indeed senior elements of both Local Authorities and the Department of Education should be using this document to challenge every single contact they may have within the providers of software to the community and saying "you are not doing a good enough job, when are you going to give us the sort of support tools that we should expect in order to provide 'privacy by design and default' as demanded by the original GDPR?" That is Satswana's true purpose, to create sufficient understanding to mobilise a clamour for change which, in turn, will mean both designing in privacy, and then delivering it by default. That will be so much more secure and save staff endless time and anxiety. We also contend that it should be far cheaper to licence, run and manage, thus creating a return for your investment in Satswana.

3 What is currently so wrong?

Put simply you have far too many pieces of information being provided to you from different places, all of which need to be fed with the same detail, which do not talk to each other. You would not do this on a paper file, you would try and write everything you needed in one place, but early computers were designed to do just one task and "specialist applications" emerged – all requiring unique staff training, with their own cost. Thus you have a MIS system that requires another program to support SEN children, neither of which includes any sort of accounting, let along budgetary control and financial management, indeed the two programs you probably use for that will not manage the payroll – that again will be separate. Add to that communication programs like Parent Mail or Studybugs – talk to Governors and you need Governor Hub apparently. Hang on, we haven't managed school meals funds yet – and so the list goes on, piling on cost, inefficiency and (in security terms) adding risk every time the information is duplicated in a different place.

4 What is the solution?

We will explain the terms below, but for those who will only read two pages we have to cut to the chase. The answer is to demand for education what every large corporate takes for granted, and that is an information system that links every aspect together in one seamless deliverable. There are no "unknowns" about this, indeed many Governors and other external influences will use such systems every day. No legal firm (for instance) would operate without a practice management system with automated billing and integrated financial reporting. Such systems are designed around a relational database structure – we explain the jargon later – which are easy to write, maintain, and (crucially) change when required. Every one of your providers knows this, but to date it has been a soft, cosy and very profitable ride for them. Nobody has really complained so they have not invested in change. The paradox is that anybody who does a better job well will clean up, so why do they hold back? Even more paradoxical some newer MIS offerings are using a relational database, but then do not include accounts – why? Perhaps the recent purchaser of SIMS will provide the answer – certainly the proposed SIMS 8 (we understood) included integrated accounting instead of FMS. To return to the comfort zone of the lay reader we should stress that we are saying that the suppliers can do it, and know how to, it is just that whilst they got away without investing in a revised product, you ended up paying and working three times as hard as you needed to. In GDPR terms, it is also massively more risky.

5 Database structures

We are going to get more technical now, but hopefully in a manner that you will feel entirely comfortable to follow. "Database" is simply the term used by computer geeks for the information held by the machine, and it is manipulated by the program to give you what you then see on the screen. Historically this was designed to run as fast as possible, providing a motorway for rapid travel through the system – it was ideal for applications such as banking and was described as being "hierarchical" – a simple old fashioned English word that means it is organised according to its rank. Just like driving on a motorway it was (is!) fast, but you cannot get off once you start, and it is not a good idea to stop – thus it is inflexible if you want to do that.

By contrast a "relational data base" is like taking a country road in that you can get almost anywhere from anywhere else, stopping when you like, changing your mind and indeed asking directions. It is very much slower doing that of course, but we are still talking very high speeds in absolute terms, certainly fast enough for any educational requirement. "RDBMS" (if you want to sound very clever!) has another feature in that you can ask it questions that were never programmed into it in the first place as in "how many children had measles in year 6 in 2017". This is described as a structured query language and you may have come across its acronym "SQL".

Thus what we should be asking the software supply industry to provide for the use of education is a program that can link everything we want to know together in one place, at one time, as we need it. Ideally that should be from one supplier, but it can also be from many, just so long as they talk seamlessly together. To say again there are no "unknowns" about this, indeed some readers may be familiar with the way Quickbooks integrates seamlessly with the Method CRM package, the Catholic Church responsible for schools in Western Australia have built an entire MIS system using just those tools. In the UK we need an exchange of information with both Local Authorities and the DfE for reporting purposes, so it is a harder task, but not insoluble.

6 Cloud systems

Moving logically forward it is likely that an integrated system would be hosted "in the Cloud" which means that you can get to it from anywhere, assuming you have a broadband connection. The real benefit here is that the cloud providers can normally provide a much higher quality level of network protection, with more skilled support staff than any school could ever afford. Having said that, as this is written, a former local authority provider has been "down" for almost a week and have not yet informed their client schools what the problem is. The lesson we fear is that it is not just the software providers who have failed to continuously update their product to the latest possible technology. It is a big challenge for the generally non-technical leadership of schools to demand optimum standards from both software providers and the related delivery infrastructure. Thus meaning that there is an open market opportunity for any organisation that can really deliver in a manner that everybody can be happy with.

7 Processors

Which brings us to the question of processors, those organisations who ask you to provide them with either your data, or access to it, in order to provide a third party service. Satswana has huge concerns over the currently casual manner in which processors are accepted. We note that one has been recommended by local authorities despite having a negative net worth of several million pounds. Can you really be confident that they are going to spend what it takes to keep your data safe? In analysing the Processor list we provide to clients we seek to consider the financial strength and the depth of the leadership as well as their compliance with an appropriate Privacy Policy. Ideally however a proper system would mean that most of these processors would not be required, creating much safer data – because clearly the more times it is stored in more places, the more the risk of an exploit must rise.

8 In summary

This paper has sought to explain in lay terms that change is required in both the quality of the software provided to education and in the manner of its delivery. The purpose of Satswana in doing so is to fulfil their mission to their customers of ensuring “privacy by design and default”. We contend that the skills exist to make the change, but corporate inertia has become too comfortable with the status quo, and that therefore the leadership within education has to demand both change and significantly lower licensing costs – together with a reduction in the training time, experience and commitment that is also so costly. The result will be safer data, less stress, better value and greater efficiency. Not demanding such change cannot be considered an option.

Appendix B

Cyber Security training for school staff

Satswana offers significant advice on training resources, but this one comes from the National Cyber Security Centre and is thus most authoritative. However, for those of you with less time a colleague recommends this three minute video! https://www.youtube.com/watch?v=i0iLy8racHI

Please note their equal concentration and concern on the subject of ransomware.

Since late February 2021, an increased number of ransomware attacks have affected education establishments in the UK, including schools, colleges and universities. In March 2021 one of the country's largest Multi-Academy Trusts sustained a ransomware attack affecting its 50 primary and secondary academies leaving 37,000 pupils and staff unable to access their email.

The National Cyber Security Centre (NCSC) previously acknowledged an increase in ransomware attacks on the UK education sector during August and September 2020. The NCSC has therefore updated this Alert in line with the latest activity.

In response the NCSC has launched a free cyber security training course to raise awareness and help school staff manage some of the key cyber threats facing schools.

The training is available in two formats: a scripted presentation pack for group delivery; and a self-learn video for staff to complete by themselves is also available on YouTube.

Find the training programme here: https://www.ncsc.gov.uk/information/cyber-security-training-schools

This available in Spreadsheet form, or copy and paste into Excel yourselves

Satswana Systems Analysis

Insert new line under each Description heading to create as much space as you require

Description	Cost	Age	Supplier	Notes (Refer to attachments if required)
Server				
Power Backup				
Network				
Operating Software				
Licences				
Diagnostic tools				
System backup				
Maintenance agreements				
Added memory				
Encryption method				
Resilience				
Firewall				
Anti Virus				
Threat intelligence				
Protection Software				
Contract services				
Consultant support				
IT contractor				
PC/Mac				
Laptops				
Tablets				
Charging systems				
Broadband				
Wifi				
Cloud systems				
Cloud licensing				
Cloud backup				
Management software				
Service backup				
Phone systems				
Printer structure				
CCTV				
Digital cameras				
Video systems				
Network conferencing				
Smart Phones				