DATA SECURITY FOR SCHOOLS

6 KEYS TO KEEPING YOUR DATA SECURE

Information technology is evolving rapidly, and threats to data security in an educational establishment are proliferating: Viruses, hackers, denial of service attacks and internal sabotage along with technology failure, natural disaster, fire, power outages, and human error. This report covers major risks, legal requirements and steps to achieve security.

DATA SECURITY FOR SCHOOLS

6 KEYS TO KEEPING YOUR DATA SECURE

Information technology is evolving rapidly, and threats to data security in an educational establishment, as elsewhere, are proliferating: Viruses, hackers, denial of service attacks and internal sabotage are just some of the threats.

But the list of security worries doesn't end there. Educational leaders must prevent data loss or corruption due to technology failure, natural disaster, fire, power outages, backup problems and human error. Of course, you must also ensure your data are kept up to date and useable.

In this environment, your duties as a school leader, department head, head teacher, bursar or administrator are complex and daunting. You must ensure your IT administrators anticipate problems and maintain legal compliance even as technology and your user needs change.

This report by Fresh Consulting will brief you on the major risks we see, current requirements under UK law and the six keys we have identified to achieving data security.

You want cost-effective and pragmatic solutions to your data security challenges. That is our specialty at Fresh Consulting. We are data security experts with extensive experience working with educational establishments. If you would like assistance assessing your system's specific weaknesses and identifying the best tools to address them, we offer a complimentary consultation. Contact us here to learn more

DISTURBING TRENDS FOR SCHOOL DATA SECURITY.

You have seen the evidence yourself of the rapid increase in data breaches, up 78% worldwide[i] in 2014 alone. The headlines are ominous:

INSIGHTS FROM FRESH CONSULTING

At Fresh Consulting, we understand the unique challenges and constraints faced by educational establishments. We are here to help you achieve data security with cost-effective and realistic solutions. Contact us for an assessment of your security readiness.

- A Staffordshire University laptop was stolen[ii] from a staff member's car and personal details on 125,000 applicants dating back eight years were compromised.
- Hackers broke into a West Sussex school's Twitter account[iii] and announced the head teacher's new "porn career," including a suggestive picture of the official.
- A school's computer network was exploited by a hacker[iv] to send a torrent of spam while concealing the true origin of the emails.
- A university student rerouted users[v] of the wireless network to a pornography site.
- First, a mother infiltrated a school district computer system and altered grades[vi] for her two children. Then a New York high school student did it himself to improve his exam scores.[vii]

These stories of malfeasance don't event touch on the serious repercussions from floods, fires, human error and back-up failure. For example:

- The Home Office lost confidential data[viii] on every prisoner in the country when the information was put without encryption on a memory stick that went missing.
- Cloud services provider Amazon Web Services had a system crash and many customers suffered permanent data loss.[ix]

LEGAL FRAMEWORK AROUND DATA SECURITY FOR SCHOOLS AND SCOPE OF THE MISSION

To grasp the data security challenge for UK schools, colleges and universities, it's important to understand the current landscape.

Government is devolving more responsibility and budget authority for data security to schools, and this is requiring school leaders to raise their understanding of security issues rapidly. Many schools are struggling to meet their IT needs in the face of budget cuts and rising educational standards.

But the costs of inadequate security can be enormous. The average organisational cost for a UK data breach was 2.37 million pounds in a 2015 study[x] by IBM and the Ponemon Institute that looked primarily at the corporate sector.

Data security consultants Gemalto calculated that every day worldwide more than 2.8 million records[xi] are exposed in data breaches. That means about 4,000 records were compromised in just the time you have been reading so far.

In the education sector, the cost of a data breach was as much as $300 per compromised record[xii] globally, Ponemon found. Schools, universities and other education organisations accounted for 8.8% of the 1.1 billion records exposed in worldwide data breaches in 2014, Risk Based Security[xiii] estimated.

Because schools hold data on students, staff, finances and other sensitive matters, they have legal responsibilities under the 1998 Data Protection Act[xiv] to keep this information as well as their IT infrastructure safe. Among the data handled by schools are names, addresses, medical information, gender, ethnicity, email addresses, telephone numbers, test results and marks.

The Information Commissioner has the power to impose monetary penalties[xv] for violations of the data protection principles. What's more, security lapses put schools and their administrators at risk for loss

of reputation and disruption of operations. Students, teachers, parents and other constituents may also face personal harm if a breach occurs.

With more than 24,372 schools[xvi] in England as well as more than 860[xvii] UK universities, colleges and other listed bodies, hackers are surely sniffing around the firewalls of many. Don't let your educational institution become one of the victims.

HOW TO MAKE SURE YOUR DATA STAYS SAFE

So how can you prevent your educational establishment from suffering a problem? We know the issues are already on your radar, and you have probably done quite a bit of work in this area.

In this section, we will focus on the best practices we have identified and deployed among the schools, colleges, academies and universities we serve.

1. **No matter how much effort you have put into your system, adopt a sceptical attitude toward your technology because it won't stay secure forever.** State of the art is a standard that is in constant motion, and hackers are working 24/7 to defeat your defences. Hewlett-Packard's Cyber Risk Report[xviii] found that most successful hacks used known vulnerabilities, and more than half exploited vulnerabilities that were more than four years old.

You become most at risk when you become complacent that your technology is doing its job.

Adopting a defensive posture will require your team to check compliance with your security policy and continuously monitor the latest hacking techniques. Is your network of printers secure? Your system and procedures will need to be adapted dynamically as threats evolve.

Similarly, don't assume you know precisely what is happening within your IT infrastructure. The news is filled with reports of breaches that were discovered months later. You may want to explore an auditing solution that gives you real-time visibility into who is accessing, downloading and sharing data. This can help you detect a breach early and highlight weaknesses that you can correct to improve your security.

Keep your guard up, deploy updates and patches, remain up to date on research, partner and collaborate with other educational organisations. If you do not have the internal resources to take on these jobs, seek out a data security expert. Fresh Consulting can help with this task.

2. **Put in place procedures to classify data and protect it**. – Many educational organisations do not have a comprehensive understanding of where their sensitive data is because they fail to systematically categorise their data. As a result, controls may not be in place to ensure that all categories of data are handled properly.

The most effective way to keep sensitive data secure is to put focus on the basics. Understand what in your data universe is sensitive, set rules for handling it, implement controls that ensure it is handled properly and train users about their responsibilities in the process.

So if your school directs that any data containing personally identifying information must be encrypted when it is moving on your network and at rest, you must first categorise your data and then implement encryption when necessary to execute your policy.

It's important to remember that user education is critical. Users need to understand the sensitivity of the data they work with and their duties in keeping it safe. That may require effort to train them in what not to do, such as downloading the data onto an insecure laptop.

If you store data in the cloud, you are putting that data on someone else's system where you do not have absolute control over it. If the data is sensitive, encrypt it before storing it in the cloud. If your cloud provider will have the key, obtain their full policies on backups, who has access to your data and what is their data breach communication policy.

3. **Secure devices and data that are leaving the building.** Laptops, tablets and smartphones enable staff to work anytime, anywhere. But it means they are taking their work and your data beyond your physical safety perimeter.

Once they leave your premises, technology and data are exposed to potential theft or loss, use by unauthorised parties (a child or friend) and use for unauthorised purposes (online shopping, for example).

Remember that this goes for senior staff too. Executives are often held to a lower standard of data security than the rest of the employees and generally have more freedom to operate outside the organisation's firewall.

But attackers are most likely to target the head or high-level official of a school because they know he or she has access to all sensitive information.

To reduce the dangers, draft and implement clear policies on technology that leaves the school. Have continuing education with staff, especially senior staff, on the issue, stressing their personal responsibility for data security.

Another area of focus is devices brought into the school environment such as mobile devices, USB drives and Bluetooth speakers which can all offer entry points for hackers. Under Bring Your Own Device (BYOD) arrangements, develop organisational standards and apply security configurations to devices and supporting infrastructure.

4. **Protect against internal threats** – When you think of security threats, your mind probably leaps to hackers, viruses, denials of service attacks and phishing.

But the greatest risk to your security most often comes from the inside. This can be a disgruntled staff member, a rogue insider or a careless and/or uninformed employee. Research by Forrester[xix] has shown that the biggest proportion of security breaches, 36%, come from employee mistakes and 25% from malicious insiders.

To mitigate this risk, adopt policies and procedures that increase organisational awareness of the problem and as well as technology that aids the effort. These include:

- Limit or prevent concurrent logins, which defends against password sharing.
- Restrict working hours or maximum session time. This makes it easier to identify when an individual has accessed the network.
- Limit users to their own work station or department. This reduces the number of computers that can be used if a user's credentials are compromised.
- Monitor user behaviour in real time so you can recognise suspicious activity.

- Respond immediately to suspicious activity even if it is a false alarm. This demonstrates to users the priority placed on security and reduces risk.
- Immediately cancel employees' computer access when they leave their jobs.
- Have a written security policy and implement continuing training and reminders about its contents.

Another often overlooked internal threat is human error, and you can take steps to prevent these. Make sure you train staff adequately, document policies and procedures that will head off mistakes (such as an explicit rule against the transfer of encrypted data to unencrypted storage), remind staff frequently of your expectations and reward employees for discovering flaws and potential improvements in your systems.

5. **Be prepared for the worst**. If you start with an assumption that someday your system will be breached, a natural disaster will strike or a server will fail, you can prepare for a swift response that will mitigate the damage and potentially halt the theft of sensitive data.

A survey found[xx] that 56% of businesses in North America and 30% of Europe did not have a disaster recovery plan, and IT downtime cost each about $150,000 a year. Another study[xxi] estimated that a single data loss incident costs on average at least $2,900.

In a crisis, your organisation will be under stress and faced with fast-paced questions and decisions that may have potentially serious consequences. Preparing in advance prevents you from having to make it up on the fly.

Draw up a disaster plan including a recovery strategy. Document protocols for immediate steps to take in the event of a power outage, natural disaster, technology failure or security violation including plans to respond to affected parties with rapid communication.

Make sure you back up your data regularly and implement additional redundancies. You never know when disaster will strike.

There is no one-size-fits-all prescription for what this should look like, but a combination of cloud storage, an automatic data backup program, archiving and servers with backup hard drives in a redundant array are commonly used.

For cyberthreats, elements of the plan should cover all phases of the response from identifying and closing off the vulnerability, reporting the breach to the Information Commissioner, remediation and other actions. There are also technology solutions that can improve your response and recovery.

You should also consider conducting risk assessments, tests, drills and incident response exercises on an ongoing basis. Being vigilant will help protect your school

6. **Keep your data up to date –** Outdated or incorrect data compromises many aspects of your operations. Under the Data Protection Act you are obligated[xxii] to ensure the accuracy of the personal data you process and that it is kept current.

To comply with this, examine your clerical and intake procedures to determine if they are sufficient to provide high levels of accuracy. Institute regular check points at which you ask people to verify their

personal details are current. Similarly, establish specific procedures for the pulling data that is no longer needed or relevant, such as when a student or employee leaves.

CONCLUSION

At this point, you might very well feel overwhelmed. This report has covered a lot of ground. Data security planning is a long-term effort, and because IT infrastructure can require significant investment, you are wise to do your research.

At Fresh Consulting, we understand the unique challenges and constraints faced by educational establishments, and we are here to help you face them with cost-effective and realistic solutions. Get in touch with us here or ring us on 020 3667 1499 to schedule your complimentary consultation.

---

[i] Gemalto NV. (2015). *2014 Year of Mega Breaches & Identity Theft.* Retrieved from http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf

[ii] Express & Star (2014, November 15). *Details of 125,000 Staffordshire University applicants on stolen laptop.* Retrieved from http://www.expressandstar.com/news/2014/11/15/details-of-125000-staffordshire-university-applicants-on-stolen-laptop/

[iii] Webb, S. (2015, March 25). *Hackers break into school's Twitter feed to announce headteacher's new 'porn career' - complete with racy picture.* Retrieved from http://www.mirror.co.uk/news/uk-news/hackers-break-schools-twitter-feed-5395784

[iv] Hansell, F. (2003, May 20). *Unsuspecting Computer Users Relay Spam.* Retrieved from http://www.nytimes.com/2003/05/20/technology/20SPAM.html

[v] Roberts, C. (2013, March 12). *Student hacks Florida University's wireless network — redirects users to porn site to expose security flaws.* Retrieved from http://www.nydailynews.com/news/national/student-hacks-school-wireless-network-redirects-users-porn-site-article-1.1286260

[vi] Grossman, S. (2012, July 22). *Mom Hacks Into School Computer System, Changes Her Kids' Grades.* Retrieved from http://newsfeed.time.com/2012/07/22/mom-hacks-into-school-computer-system-changes-her-kids-grades/

[vii] Whitelocks, S. (2015, February 27). *Tech-savvy student, 16, arrested after 'hacking school computer system to improve his grades.* Retrieved from http://www.dailymail.co.uk/news/article-2972270/Tech-savvy-student-16-arrested-hacking-school-computer-improve-grades.html

[viii] Winnett, R. (2008, August 21). *Home Office loses confidential data on all UK prisoners.* Retrieved from http://www.telegraph.co.uk/news/uknews/law-and-order/2598204/Home-Office-loses-confidential-data-on-all-UK-prisoners.html

[ix] Blodget, H. (2011, April 28). *Amazon's Cloud Crash Disaster Permanently Destroyed Many Customers' Data.* Retrieved from http://www.businessinsider.com/amazon-lost-data-2011-4?IR=T

[x] Ponemon Institute LLC. (2015). *2015 Cost of Data Breach Study: United Kingdom.* Retrieved from http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03054GBEN&attachment=SEW03054GBEN.PDF

[xi] Gemalto NV. (2015). *2014 Year of Mega Breaches & Identity Theft.* Retrieved from http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf

[xii] Molnar, M. (2015, June 2). *Data Breaches Cost Education Companies $300 Per Record, Study Finds.* Retrieved from http://blogs.edweek.org/edweek/DigitalEducation/2015/06/data_breaches_cost_education.html

[xiii] Risk Based Security, Inc. (2015). *Data Breach QuickView 2014 Data Breach Trends.* Retrieved from https://www.riskbasedsecurity.com/reports/2014-YEDataBreachQuickView.pdf

[xiv] British Educational Communications and Technological Agency. (2004). *Data protection and security- a summary for schools*. Retrieved from http://cnp.naace.co.uk/system/files/data_protection_in_schools.pdf

[xv] Information Commissioner's Office. (2012). *Report on the data protection guidance we gave schools in 2012.* Retrieved from https://ico.org.uk/media/for-organisations/documents/1132/report_dp_guidance_for_schools.pdf

[xvi] Department for Education. (2014, January 10). *Number of schools, teachers and students in England.* Retrieved from https://www.gov.uk/government/publications/number-of-schools-teachers-and-students-in-england/number-of-schools-teachers-and-students-in-england

[xvii] British Council. (n.d.). *Universities and colleges.* Retrieved from http://www.educationuk.org/global/articles/higher-education-universities-colleges/

[xviii] Prince, B. (2015, February 23). *Old Vulnerabilities Still Popular Targets for Hackers: HP.* Retrieved from http://www.securityweek.com/hp-cyber-security-report-reveals-old-vulnerabilities-still-popular-targets

[xix] Shey, H., Balaouras, S., Luu, B. & Mak, K. (2013). *Understand The State Of Data Security And Privacy: 2013 To 2014.* Retrieved from https://www.forrester.com/Understand+The+State+Of+Data+Security+And+Privacy+2013+To+2014/fulltext/-/E-RES82021

[xx] Harris, C. (2011, May 24). *IT Downtime Costs $26.5 Billion In Lost Revenue.* Retrieved from http://www.informationweek.com/it-downtime-costs-$265-billion-in-lost-revenue/d/d-id/1097919?

[xxi] Smith, D.M. & Williams, M.L. (n.d.). *Data Loss and Hard Drive Failure: Understanding the Causes and Costs.* Retrieved from http://www.deepspar.com/wp-data-loss.html

[xxii] Information Commissioner's Office. (n.d.). *Keeping personal data accurate and up to date (Principle 4).* Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/