THE BURSAR'S REVIEW

Summer 2015

The Official Magazine of the ISBA

# ESOS

## is here...

and it's mandatory,
**we make it easy**

Page 27

**BUILDING CYBER SECURITY**

Page 45

**ISBA CONFERENCE – Sharing knowledge and ideas**

Page 32

**PLUS: HOW THE CDM REGULATIONS 2015 WILL AFFECT YOUR SCHOOL**

I·S·B·A Independent Schools' Bursars Association

Author

Francisco Ordillano
consulting partner and commercial director, Infosec Partners Ltd
www.infosecpartners.com

# BUILDING CYBER SECURITY

**The 'big bad wolf' is real, motivated, and actively targeting the personal, sensitive and financial information that your school holds.**

Once upon a time, there were three little pigs. One pig built a house of straw while the second pig built his house with sticks. The third little pig worked hard all day and built his house with bricks.

We're all familiar with this story and its moral of how building with the right foundations and materials can provide a secure future. All the best independent schools are founded on principles and vision and it's their reputation that attracts families who want to give the best possible start to their children, including those of high net-worth and influence.

The world is increasingly interconnected and schools are right to embrace the many efficiencies and benefits afforded by technology. Mobility, online education, cloud, WiFi and BYOD (where staff and pupils choose and bring their own devices to access resources) are rapidly becoming the new normal for schools, as they are already in other sectors. However, as news of organisations being hacked becomes commonplace, there are several significant concerns for schools who face growing cyber security threats and need solutions to overcome the new challenges of protecting children in their care.

## Resources at breaking point

There has been an exponential increase in the responsibilities of the average school IT manager. How can they maintain and support the growing demands of pupils and staff as well as hold expertise on something as critical, fast changing and complex as cyber security? Often the answer is that they cannot. Fire fighting (the process of dealing with the highest priority problem first amidst lots of shouting, wailing and general gnashing of teeth) is all too familiar for school IT managers, especially for those with limited budgets.

Outsourcing the school's IT systems maintenance and support has become a popular way to try and balance the need for skilled resources and limited budgets, however, the vast majority of the service providers are simply not skilled, certified or knowledgeable enough to be able to ensure the comprehensive security which schools need. A recent article in TeachingTimes.com recommends, "Dedicated security companies that manage the latest technologies to combat cyber threats are worth considering..."

## Schools are targets for a variety of predators

A big bad wolf saw the two little pigs while they danced and played and thought, "What juicy, tender meals they will make!"

With security awareness and defences relatively high in the large enterprise organisations that are worked for, led, or owned by pupils' parents, attackers always look for the weakest link. Attackers are motivated and can vary from those wanting to steal financial records or those looking to exploit personal information for ransom, to undesirables.

Schools have a responsibility to prevent children from visiting adult, illegal or otherwise inappropriate websites and inspections and audit guidelines relating to eSafety have focused mainly on protecting children from being exposed to this content.

Predators lurk within social media chatrooms and games, and many cyber safety-awareness programmes teach children not to give out their personal information, but cyberbullying also uses this media and is another significant threat. There is a false sense of anonymity associated with cyberbullying, suggesting that 'online is not real life' and that this means the perpetrators cannot be identified or brought to account.

Unfortunately, the effects of bullying online can be just as bad, if not worse than bullying in person.

The New York Times recently posted a report regarding how an app, which allows localised groups of people to post instant messages anonymously for other people in the same area to see, on whatever subjects they want, has already been used to "issue threats of mass violence on more than a dozen college campuses" in the US, as well as proposing a gang rape at a school's women's centre.

The big bad wolf went to the first house and huffed and puffed and easily blew the house down. The frightened little pig ran to the second pig's house that was made of sticks. The big bad wolf went to this house, huffed and puffed and quickly blew that house down. Now, the two terrified little pigs ran to the third pig's house made of bricks.

Schools hold data belonging to pupils and their families, such as health and attendance, performance and disciplinary issues etc. Schools may also be privy to additional personal information regarding sensitive family issues.

Consider the following two scenarios:
**RISK 1.** A child sees adult pornographic material on a computer whilst at school.

**RISK 2.** The school's main curriculum server is hacked by a disgruntled ex-service provider, they take information relating to a child's illness, details of treatment, and psychological issues involved, and then post the details on the internet with copies of formal documents, photographs, etc. The information is then sent, along with evidence of fees paid, details of bank accounts and personal data to the parents threatening to release their and other children's data to the public.

continued on page 46

continued from page 45



Modern networks **must be resistant** to modern threats

News of organisations **being hacked is commonplace**

The **effects of bullying online** can be just as bad, if not worse than bullying in person

The loss of sensitive personal data may have a far greater social and psychological impact on the young and vulnerable, concluded a report from as far back as 2008 when renowned psychologist, Tanya Byron, was engaged by the prime minister to write a report focused on the emotional impact of technology in schools.

## Straw and twigs V bricks

Typically, over time, technology is added to a schools' network infrastructure to meet each new security need. From funding to manageability, there are several problems related to buying technologies from many vendors. Maintenance costs alone can be expensive especially with many vendors choosing a per-seat model to charge for licensing. Running costs such as electricity, cooling and rack space adds up with each appliance on the network. Having different devices with different interfaces also means more time learning about and trying to keep on top of it all, which is time lost that could otherwise be spent supporting school projects.

With the majority of today's attacks using multiple vectors, having disparate point solutions for each requirement could leave the whole collection unaware of blended attacks, and effectively, leave your school defenceless. Modern networks must be resistant to modern threats. Bursars, heads and governors should be worried about security, the potential loss of sensitive data belonging to students and their families, as well as that of the school such as financial data and interim, unpublished results of inspections, or HR issues with previous or existing members of staff.

The Data Protection Act and regulators have caught up, auditor guidelines are being strengthened and security vendors are providing secure solutions, however many schools have not yet begun to suitably address security.

The big bad wolf tried to blow the third house down, but he couldn't. The house was very strong and the little pigs were safe inside. He tried to enter through the chimney but the third little pig boiled a big pot of water, kept below the chimney, which the wolf fell into and died.

## The moral of the story?

By building upon a well-designed information and cyber security strategy, enabled by a combination of policy and best-of-breed integrated security technologies, schools can easily have the protection they need to fend off the increasing threats…and live happily ever after.

CHECK LIST

# TOP 5 CYBERSECURITY CONCERNS FOR SCHOOLS

*As news of organisations being hacked becomes ever more commonplace, Infosec Partners highlights 5 concerns for schools facing increasing cyber security threats and provides solutions to overcome the challenges of protecting children in their care.*

### DUTY OF CARE

Schools are charged with the duty to protect children in their care, but how can they provide this given the increasing dependence on connectivity, as well as the use of the Internet as part of the standard learning approach?

### STAFFING & EXPERTISE

Attracting and keeping hold of talent is an arduous enough task for the large Enterprise, so how are schools supposed to ensure they have expertise on-hand, especially for something as critical, fast-changing and complex as cyber security?

### FUNDING

As any Bursar or Headmaster will know budgets are becoming increasingly squeezed, so how can one equate the spend on security solutions with benefits to the school, especially when all areas are clamouring for more funding?

### MOBILITY & THE NEW NORMAL

How can the IT department secure and support students, faculty and staff in the new normal of mobile use, online education, cloud and BYOD?

### REPUTATION

From competitive state run schools to exclusive globally recognised independent brands, how can schools protect their reputation from the potentially catastrophic impact of a cyber attack and exposure of sensitive information?

## NEXT STEPS

Worried about the cybersecurity threat to your school? Contact **InfosecPartners** for trusted advice and expertise today.

**Call** 0845 257 5903