THE BURSAR'S REVIEW

Spring 2016

The Official Magazine of the ISBA

FLOURISHING PARTNERSHIPS

BETWEEN INDEPENDENT AND STATE SCHOOLS

Page 10

A PRACTICAL APPROACH TO THE GODDARD INQUIRY

Page 28

HIDDEN PREDATORS ARE AFTER YOUR DATA

Page 50

PLUS: THE ISBA HR CONFERENCE **PAGE 37**

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

Author

Francisco Ordillano, communications director at Infosec Partners

www.infosecpartners.com

WHO CRIED 'WOLF'?

Once upon a time, a shepherd boy, who watched a flock of sheep near a village, cried "wolf wolf!"

Amidst all the noise, can your school demonstrate that it is able to provide suitable safeguarding for its pupils and be able to act upon a genuine cry for help?

A wolf in sheep's clothing?

The passing of the Counter-Terrorism and Security Act 2015, which puts a responsibility on schools to prevent pupils from being drawn into terrorism, underlines again that we live in a rapidly changing world where today's 'big bad wolf' might appear differently to previous manifestations.

In May 2015, the Guardian newspaper published an article interviewing the UK's most senior Muslim police chief. As a parent as well as Scotland Yard commander, Mak Chishty warned that what was new about Islamic State (Isis) is its use of social media and the internet to spread its message and urge people to join the group or stage attacks in their home country. "We are facing a risk, a threat which is global, which is powerfully driven by social media, reaching you on your own through your mobile phone."

The internet, accessibility of mobile devices and the ease of communication we enjoy today are now being extensively utilised by a variety of predators. From cybercriminals who are looking to steal your school's information for profit, to paedophiles, bullies, and those spreading extremist ideals on social media, there is much to be vigilant about and 'safeguarding' which is at the heart of the new Common Inspection Framework (CIF) attempts to address this.

An article in FEWeek.co.uk last October by Paul Joyce, a deputy director at Ofsted, highlighted that inspectors are called upon to ask a range of questions to evaluate if the school has effectively assessed the risk to its pupils safety.

- Do the pupils feel safe?
- Do staff understand the range of risks to pupils and would they recognise signs of cyberbullying, child sexual exploitation or vulnerability to extremism?
- Would staff and pupils know where to refer such cases where they have concerns?
- Could the school demonstrate where they effectively handled an incident?
- What about recruitment? Has the school put necessary and proportionate steps in place to ensure proper vetting of potential staff?
- What steps have schools taken to review cases and policies?

Evaluating the level of awareness, the capability of noticing changes in behaviour and the ability to act are at the core of these questions, and it is the responsibility of the school to explain how their answers are put into practice.

Identify a wolf by its behaviour

The challenge for many schools is to understand how to translate policies into actual security controls. Schools are now used to the idea that we need to protect children from exposure to harmful content on the web, and content filtering systems have been used by schools to block websites categorised as having harmful or unsuitable content, such as pornography and violence.

However, the need for prevention has turned into the need for monitoring behaviour and activity. It is no longer good enough to just block and this raises a challenge. While many systems used by schools track activity down to network IP address, it is imperative that all activity is accurately matched to an authenticated user.

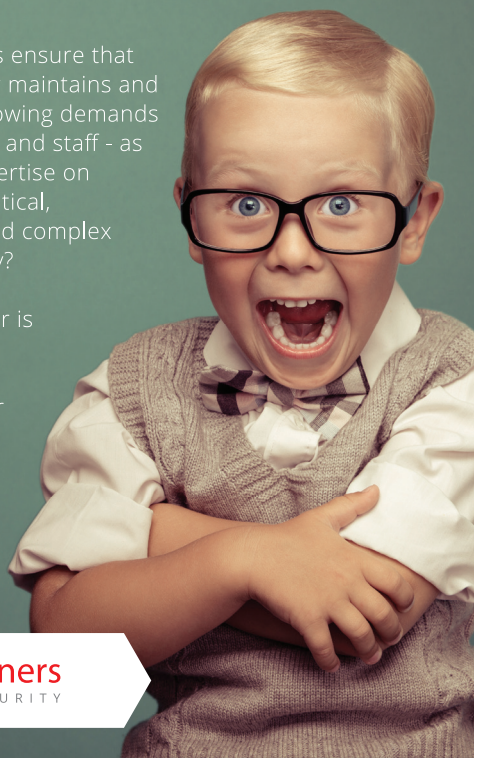
continued on page 52

UNDER ATTACK

Are your resources at breaking point?

How can schools ensure that thier IT manager maintains and supports the growing demands of pupils, faculty and staff - as well as hold expertise on something so critical, fast-changing and complex as cyber security?

Often the answer is they cannot. Contact Infosec Partners now for proven security support and trusted advice.



InfosecPartners
CYBERSECURITY

FORTINET

Save and Secure with Fortinet for Schools

Typically over time technology is added to a school's network infrastructure to meet each new security need. From funding to manageability, the cost of a patchwork network can be very costly.

Integrated security from Fortinet eases the worries on your safety and your budget.

InfosecPartners
CYBERSECURITY

FORTINET
PARTNER OF EXCELLENCE

CHECK LIST

Assessing your RISK

How effective are you?

With the new common inspection framework, Ofsted and ISI inspectors are called upon to ask a range of questions to evaluate if the school has effectively assessed the risk to pupil safety.

ADDRESSING THE CHALLENGES

At Infosec Partners we believe there are several fundamentals that each school needs to address in order to be able to suitably secure the school and it's pupils, and subsequently pass inspections.

- ☑ **CROWN JEWELS EVALUATION** - The theft, misuse or corruption of critical or sensitive data can cripple operations, severely damage brand reputation, and dramatically impact the lives of pupils, families or staff.
- ☑ **SECURITY RISK ASSESSMENT** - Includes an evaluation of specific risks and threats, categorising information assets and agreeing which need the most protection and which require less stringent controls.
- ☑ **GAP ANALYSIS** - This evaluates whether the controls in place, including both policies and technologies, are suitable and measurable against compliance and security standards.
- ☑ **PRIORITISED ACTION PLAN** - Actions to remedy any gaps identified should be prioritised against the results of the security risk assessment. It's as important to be able to reason why you don't have a particular control in place as list the ones you do.

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

schools@infosecpartners.co.uk 0845 257 5903
visit: http://schools.infosecpartners.co.uk

continued from page 50

Wolf hunt

Safeguarding is at the heart of the new Common Inspection Framework

All activity must be **accurately matched** to an authenticated user

More intrusive applications provide a much larger haystack of data to review

In the new normal, where pupils and faculty staff are more mobile (working away from school), bringing and using non-standard devices (BYOD) or utilising online education tools stored in the cloud, it is a much larger task for schools to keep children safe, let alone stay in control and monitor activity. And with search engines like Google now employing HTTPS (a protocol for secure internet connections) as a standard, web searches are now encrypted resulting in a need to decrypt traffic in order to monitor activity.

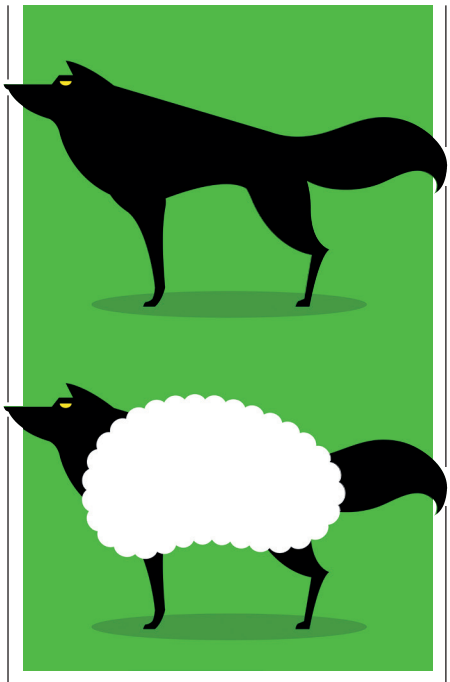
Which one of you cried 'wolf'?

Many schools still operate a patchwork set of security solutions by different vendors as typically, over time, technology is added to a school's network infrastructure to meet each new requirement. Unless using integrated security solutions from a single specialist security vendor, or using a cleverly integrated event/log correlation solution to combine the information generated by each tool, then schools will not get to see the big picture and cannot provide the monitoring required through all the 'noise' each tool generates.

However, even if you work with well-integrated security controls, the number of alerts and data to review can be difficult to wade through and act upon. Well-defined process, a rugged security framework and security expertise (which schools typically lack in-house) are all needed to ensure that critical warnings and symptoms do not get lost amidst all the noise.

How schools should address the challenges

It is important for schools to have a risk assessment including an evaluation of their specific threats and risks, identifying and agreeing what they feel is important for them i.e. those things that need the most protection, and what is less important and requires less stringent controls. A gap analysis would then evaluate whether the controls in place, including both policies and technologies, are adequate or if they need to be enhanced, improved upon or replaced. Gaps that do exist must be addressed and must have a suitable control identified and implemented, but being able to explain why you have chosen not to have a particular control is as important as being able to list those that you do.



With 'best of breed' network-based security, schools can achieve a good level of visibility into the network activity of pupils, faculty and other staff. Through security controls, including age-appropriate content filters and correlation of web searches and individual webpage activity identified through features such as SSL Deep Packet Inspection (which gives the ability to see inside encrypted network traffic), Data Leak Prevention (which gives the ability to monitor the sharing of sensitive information) etc., schools can satisfy both the protect requirement and Ofsted/ Independent Schools Inspectorate's audit requirements for safeguarding.

There are more advanced security controls that have recently become popular which give even more visibility into everything that is typed, viewed or accessed on any device. However, while these more intrusive applications can give additional information, they also provide a much larger haystack of data to search through and review.

This also introduces additional risks and exposure for both the school and the pupils around data protection and human rights when you can view, record and search for their most sensitive information such as medical data, personal family messages and so on.

It is usually only those mature security organisations with a robust security strategy and a high enough level of experience in their security platform, that feel the need to go to this extra level of control. For most, these intrusive tools bring with them far more risk than they remove.

Act now

The wolf did truly come at last. The shepherd boy, now really alarmed, shouted in an agony of terror "come and help me. The wolf is killing the sheep!" But no one paid any attention to his cries, nor gave him any assistance. The wolf, having no cause for fear, destroyed the whole flock at his leisure.

The moral of the original 'boy who cried wolf' story is of course simply that 'nobody believes a liar even when they're telling the truth'.

But, there are several additional warnings for the village elders/school leaders about being able to identify and act upon a real attack, while simultaneously being able to protect the children from whatever dangerous behaviour the predators are grooming them to enact. In light of recent social and political developments and the direct evidence of growing threats to children of a school age, the new Common Inspection Framework's focus on safeguarding as an activity, means it is imperative that schools have a comprehensive understanding of the risks they face and what they are doing to counter them.

> "Even if you work with well-integrated security controls, the number of alerts and data to review can be difficult to wade through"