How cybersecure are EdTech products in the classroom?

By Velislava Hillman

As part of an international working group that aims to develop cybersecurity standards for the EdTech sector, Dr Velislava Hillman, visiting fellow at LSE, argues that products like Microsoft Teams were never meant for children and discusses the risks that EdTech products' security vulnerabilities may expose them to.

When Covid-19 lockdowns led to many schools going virtual overnight, Swen, a software developer from Germany, knew his children had no choice; their lessons carried on via Microsoft Teams. Swen quickly realized the product's security problems: "You can literally set up your own free Outlook account, simply log in on Teams and connect with students like in any other chat platform without restrictions."

What are the cybersecurity risks with EdTech software?

Most software is developed with businesses, not children in mind. Android systems, for example, any programmer can exploit its vulnerabilities and create so-called remote code executions (RCE), which bypass the user level and go to the root level of their device to gain control over it. This reflects a general vulnerability with the operating system (OS), allowing an attacker to exploit a known common vulnerability exposure (CVE) in a device's media player. It is sufficient to include this vulnerability in an MP4 (a common video file), disguise it as a funny cat video and send it to a child. Once played, the video loads malware and takes control of the device.

Such cybersecurity vulnerabilities are everywhere. The popular online gaming platform Roblox allowed an individual to hack its gaming protection systems in order to customize how animations appear, allowing a 7-year-old child's avatar to be raped. Strangers can hack children's smart toys because of security flaws. In the EdTech sector (Figure 2), cybersecurity incidents are rampant. Education data breaches continue to grow, as shown in Figure 1.

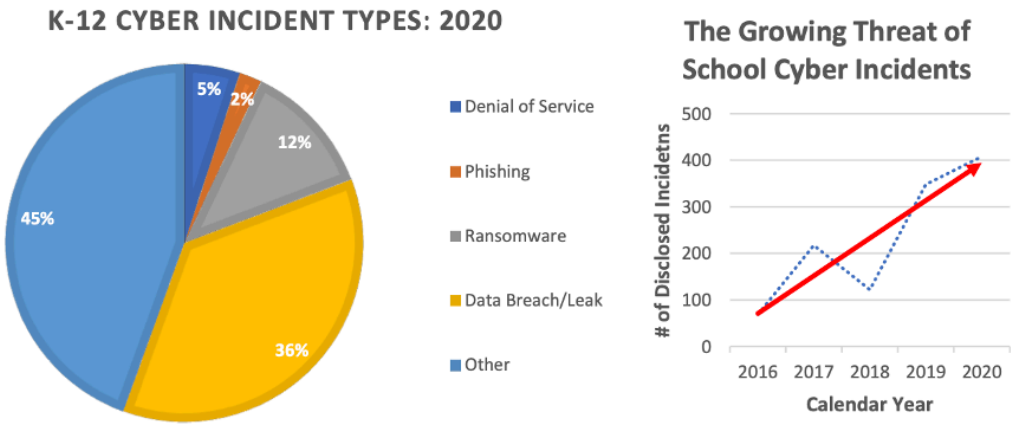

Figure 1: Cybersecurity incidents in American schools

"It is very easy to carry out RCEs or privilege escalation on older devices running older versions of a mobile operating system", says Swen. These translate as the act of exploiting a bug or a vulnerability in a system to obtain unauthorized access to it. When installing a new application or software on the phone (Apple or Android), the device owner is typically asked to provide a password before such a 'root change' is executed. This is a user privilege; cybersecurity vulnerabilities mean that this privilege can be bypassed.

Other forms of software vulnerability exist even without exploiting a user's device. Snapchat, the social media application, notifies users when another user screenshots the sender's photo or messages in the app, but users can circumvent this feature. Snapchat hides the photo from the smartphone's screenshot feature, using a simple overlay of the software. However, by installing third-party applications, a user can remove this overlay, trick Snapchat and still take a screenshot. Incidentally, Google generated over four million results for the 'Snapchat screenshot hack'!

Image credit: Hquality, from Shutterstock

What questions should schools ask to assess cybersecurity in the EdTech they use?

1. **What are the software features?**

Does the application enable the exchange of images and communications? Does it necessitate the use of microphones and cameras where the software is installed? In short, can other people get in touch with the pupils just by chatting? Is it possible to extend the features just by installing or activating additional packages? If so, can this be denied by an administrator? What are the sources of those packages? If new features are added by the EdTech operator, can the user (pupil or parent/guardian) disable any of them or switch them off? The Age-Appropriate Design Code enforces digital products to place default settings on 'high privacy' – and thus to turn various features 'off' by default.

2. **Who is the EdTech operator and is there a single point of contact?**

This is a tricky question as many start-ups are acquired by bigger businesses or may change names. When the for-profit Chan Zuckerberg Initiative's Summit Learning school platform caused parental concerns about student privacy, the company changed its name. Start-ups may also be acquired by other companies. Providence Equity Partners acquired Blackboard, the virtual learning environment. Kahoot, the game-based learning platform, acquired Clever, the single sign-on platform that manages more than 65,000 schools' data (while using Amazon Web Services!). Globally acquisitions in the EdTech sector are rife, frequent and hard to follow. Not knowing who the software owner is, means it is hard to know who will address your complaints. It is, therefore, in schools' and children's best interests that schools identify and establish contact with the software owner before deploying the software for children to use.

3. **How often is the software updated?**

The frequency of software updates matters greatly; it means that the software responds to 'bugs' – vulnerabilities that open doors to cybersecurity threats. Examples aplenty – not only among start-ups but also among behemoths like Microsoft who don't always update software regularly. For example, Microsoft didn't update an RCE bug that was 'wormable' (via a program that can distribute itself to other machines on a network). The result was a widespread virus called *wannacry*– ransomware that encrypts a computer's data and decrypts it after payment is made to the hijacker. Google, too, has issues with their Android system. A long-lasting vulnerability that was open for years is CVE-2018-21042, an RCE bug that is delivered right through the device's messenger functionality. Today, while nearly 70% of the world's population uses Android, this bug is still not patched. This opens doors for cybersecurity threats such as unauthorised access to accounts or taking control over one's Android device.

Though there is no EdTech specific security standards, EdTech providers should strive to comply with international standards for Information Security Management Systems (ISO/IEC 27001) and its privacy extension (ISO/IEC 27701:2019). Providers of EdTech services that involve direct interaction with child users should also seek compliance with the IEEE standard for an Age Appropriate Digital Services Framework. While these standards are voluntary, compliance will likely build trust in EdTech products and services.

What can schools do?

While children have no real choice in school about the technologies they must use, it is important that schools who procure these technologies, parents and children who are using or exposed to these technologies in schools are aware of these tools' limitations. Swen believes that children should be taught to understand the potential security risks of the technologies they use daily to advance children's digital literacies.

Applying the basic cybersecurity vulnerability assessment: Examples of three EdTech products

Site	Tracking engagement and/or location	Communication features	Chat with unknown parties	Single point of contact	Providing help with software functionalities and features	Comment
Dr Frost	Yes	Yes	No	Yes	No	This is a typical example of an EdTech: teacher-to-class kind of teaching children in maths. Unfortunately, the service offers no helpdesk or documentation to get a proper overview of features.
Kahoot!!	Yes	Yes	No	Yes	Yes	There is a lot of gamification built in, which can be a problem because students can get distracted; from security point of view they look fine; the company has been around for a while.
Class Dojo	Yes	Yes	Yes	Yes	Yes	Similar to Kahoot, there are some features that offer access for other users to get in touch with the pupil user.

Having applied this assessment, schools can decide whether the risks are worthy of the benefits the software in question can provide and how to manage these risks. That said, the responsibility to identify, mitigate and manage these risks belong primarily to EdTech providers to make their products and services secure by design and respectful of children's rights.

Velislava Hillman is a Visiting Fellow at LSE and founder of EDDS, where she leads an independent team of international experts providing comprehensive audit and evaluation of education technology operators. As a researcher and academic Dr Hillman's work lies in education focused on the integration of AI systems into schools and the role and participation of children and young people in increasingly digitalised learning environments. Through EDDS, Dr Hillman maintains two objectives: to develop minimum standards and benchmarking of the edtech sector, and to offer a unique enhanced reporting mechanism that gives students, parents and educators peace of mind when choosing and using education technologies.

Originally posted on https://digitalfuturescommission.org.uk/ on March 21, 2022 .