Education:

Securing your network against cyber breaches

swivelsecure

Contents

Introduction

Education

Recent years have seen our classrooms become increasingly connected. With advances in technologies such as smart devices and cloud computing, students now have better access to learning tools and resources than ever before.

But despite the benefits on offer, connected classrooms pose a cybersecurity risk.
For Education facilities, protecting IT systems and applications is crucial for the safeguarding of students and staff.

Additionally, the issue is further complicated by some serious challenges in the sector, including a lack of IT funding, a lack of clear policy, and insufficient training across the user population

At Swivel Secure, we protect Education facilities around the world with our cost-effective range of solutions including multi-factor authentication.

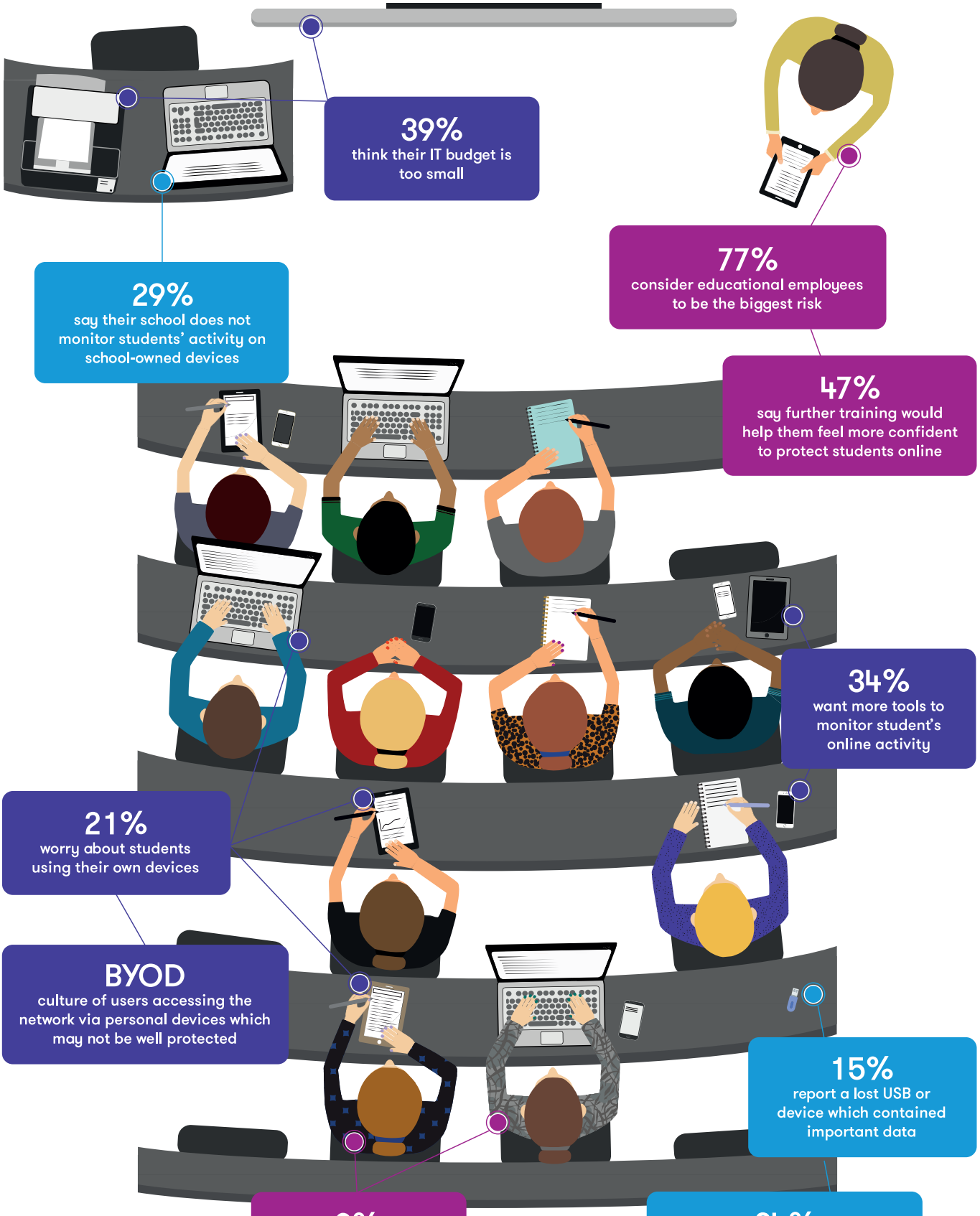
Read on to find out how you can help secure your Education network against cyber breaches.

Infographic

Higher Education under threat to cyberattacks

Higher Education venues are a prime target for hackers. In the past 2 years, attacks have doubled with 1,152 taking place between 2016-17, according to The Times.

As the classrooms become more digitally connected, IT professionals need to work even harder to secure their network. Take a look at our infographic to see the biggest risks and concerns according to educators.



39%
think their IT budget is too small

77%
consider educational employees to be the biggest risk

29%
say their school does not monitor students' activity on school-owned devices

47%
say further training would help them feel more confident to protect students online

34%
want more tools to monitor student's online activity

21%
worry about students using their own devices

BYOD
culture of users accessing the network via personal devices which may not be well protected

15%
report a lost USB or device which contained important data

3%
of students are trained in cybersecurity

34%
say that data loss is one of the biggest areas of concern for their school's IT security

52%
want more cybersecurity training for students

Article

Why Cybersecurity needs to be a priority for the education sector

Education institutions need to make cybersecurity a priority. Despite the sector facing major challenges such as a lack of staffing and a lack of funding and resources, cyberattacks are no less frequent or less severe in education. In fact, they seem to be gaining ground in prevalence year-on-year as instances of breaches in schools and higher education are widely reported.

In recent years we've seen news of ransom attacks causing financial damage – like that on the University of Calgary where the institution allegedly handed over $20k to cybercriminals, and malware attacks causing mass disruption – similar to the disruption which, apparently, caused the Minnesota School District to shut down for a day while IT professionals rebuilt the system.

We've also seen more worrying breaches where student safety is compromised. Educational institutions are entrusted to safeguard their students, many of whom are minors, but a weak cybersecurity infrastructure can put them at risk.

This was made all too clear when the CCTV in several schools in Blackpool was allegedly breached, and the footage reportedly live-streamed on the internet.

It's an unfortunate fact that, while cybersecurity in education is necessary to protect against financial loss and prevent disruption, it's also crucial to protect students from harm.

Which is why the sector needs to do everything it can to ensure their applications and systems are protected, and work to overcome challenges.

In this article, we'll look at the current state of cybersecurity in education. We'll discuss the most common reasons for attack, the highest threats and the main challenges facing the sector to help you understand why cybersecurity needs to be a priority, and how you can make it a priority for your educational institute.

Why Education is a target for cybercrime

There are four key reasons why Education is a target for cybercriminals.

With Education venues varying in size, purpose, and stature, the motives for attack can vary too. For example, what might be a common threat for world-renowned Universities/Colleges might not be an issue for schools or school districts. So, institutions need to evaluate the risk and understand what data is vulnerable to unauthorised access.

DDoS attacks – Distributed Denial of Service, or DDoS attacks are a common type of attack on all levels of Education venue. This is where the attacker's motive is to cause widespread disruption to the institute's network, having a negative effect on productivity.

This can be a relatively easy attack for amateur cybercriminals to carry out, especially if the target network is poorly protected. There have been instances of students or teachers successfully carrying out a DDoS attack, with motives ranging from simply wanting a day off, to protesting the way a complaint was handled.

Continued >>

Data theft – This is another attack affecting all levels of education because all institutions hold student and staff data, including sensitive details like names and addresses. This type of information can be valuable to cybercriminals for several reasons, whether they plan to sell the information to a third party or use it as a bargaining tool and extort money.

The concerning aspect of this type of attack is that hackers can go unnoticed for long periods of time. As was the case at Berkeley, where at least 160,000 medical records were allegedly stolen from University computers over a number of months.

Financial gain – Another motive for hackers carrying out an attack on an education institution is for financial gain. This might not be as high a risk for public schools, but with private institutions and Universities/Colleges handling a large number of student fees, they're a prime target for cybercriminals.

Today, it's usual for students or parents to pay fees via an online portal, often transferring large sums of money to cover a whole term or year of tuition. Without proper protection or preparation on the part of education institutions, this presents a weak spot for cybercriminals to intercept.

Espionage – The fourth reason why education is a target for cybercrime is espionage. In the case of higher education institutes like Universities/Colleges, they're often centres for research and hold valuable intellectual property.

Universities/Colleges need to be suitably protected, as it's thought that scientific, engineering and medical research by UK Universities has been previously compromised by hackers, and with plenty of time and money to fund them professionals are often at the helm of these attacks.

With these four motives in mind, the way in which hackers carry out an attack on Education networks can further help us understand how to protect them.

How Education is targeted

JISC's 2018 Cybersecurity Posture Survey questioned IT professionals within further and higher education. They were asked to name the top cyber threats facing their institutions, and the top three answers give us insight into the most common ways Education networks are breached.

Phishing – Phishing scams often take the form of an email or instant message and are designed to trick the user into trusting the source in a fraudulent attempt to access their credentials – whether that's sensitive student data or confidential research.

This type of attack is highlighted as the top threat facing higher education venues, suggesting hackers regularly target the sector using the method.

Ransomware/Malware – Also in the top three cyber threats highlighted by the report, ransomware and malware attacks prevent users from accessing the network or files and cause disruption. More advanced forms of this threat can see attackers hold files to ransom.

Ransomware or malware typically infects devices using a trojan, a file or attachment disguised to look legitimate. However, some ransomware (like the WannaCry attack) have been shown to travel between devices without user interaction.

Lack of awareness – The third threat listed by professionals in both further and higher education is a lack of awareness or accidents. This could be on the part of staff or students who aren't sufficiently trained to practice good cyber hygiene or accidentally compromise the network.

Despite taking on different appearances, human error plays a key part in each of these three Education sector cybersecurity threats. However, with better overall cybersecurity training, and awareness on the motives and method of attackers, education venues could better protect themselves against cyberattacks.

However, the sector is also facing challenges which hinder progress.

The challenges Education is facing

The JISC report also investigates the challenges facing IT professionals when it comes to protecting Education networks. When asked to rate how well their institution is protected on a scale from 1 (not at all) to 10 (very well), further education scored lower overall than higher education. The mean score for further education institutions was 5.9, while higher education scored 7.1.

The rationale behind lower scores included:

- A lack of resources and budget – potentially pointing to the lack of finances to invest in cybersecurity, be it software or staff.
- Cultural issues – a 'Bring Your Own Device' culture is common in Educational institutions and can present difficulties in securing the wider network, particularly with IT staff already facing stretched resources.
- An absence of policy – setting out policies for using the network and making sure they're adhered to can be difficult in large institutions with a dynamic user population.

Despite these challenges, the Education sector is still expected to secure their networks against unauthorised access and cyber threats. Especially when the repercussions can be as severe as the examples we discussed earlier.

But there are some critical steps every institution should undertake to lay the foundations for a secure IT network.

Reducing the risk to the Education IT network

With the challenges of poor funding and a lack of resources, the Education sector should focus their efforts on minimising the risk of a cyberattack, rather than a reactive attitude after one has happened.

Training

Providing basic training for all users of your network is one way to mitigate the effects of a lack of funding and resource.

This can be something as simple as sharing a handbook with staff and students including information about what to look out for, and tips for practising good cybersecurity hygiene. Giving people the necessary information to protect the network at all access points, could reduce the number of incidents caused by human error.

Authentication

Another cost-effective way to protect the safety of your institution and its students is to implement a user-friendly multi-factor authentication (MFA) tool.

Including that extra security step for users who are logging onto the network will help prevent unauthorised access. An easy-to-use platform should be high on your list of things to look for in an MFA provider.

If users can use a platform self-sufficiently, there's less likely to be a need for administrative support, so education facilities can save on overheads without compromising network security.

These are just some of the cost-effective ways to protect your School, University or College from any form of unauthorised access. With the increasing frequency and potential severity cyberattacks pose to the Education sector, it's crucial that IT professionals can work to find a solution to challenges like a lack of funding.

Interview

Top tips for securing your Education network

Andrew Donaldson, regional manager for Swivel Secure, and Adrian Jones, CEO, discuss how education facilities use their IT systems and networks. They looked at the common cyber challenges the industry faces and offer their advice for securing an education network.

Andrew: So Adrian, what dœs a typical IT network look like in an educational facility?

Adrian: I don't think there is a typical network in an educational facility. They are so diverse and there are so many different versions of it. It's been around for a very long time.

They were the first people to build the web and the Internet and they grow in that with all of their systems, whether it be POS or whether it be internal systems, email.

Capture the QR code to see the full video.

The Internet itself was based on the education market from the military. That was the first place where it expanded. So they're so diverse, they're so complicated and they're so different.

And it's the same thing with the user community. They are totally different between facilities. You've got staff members and then you've got students, right the way through to pupils - and they can be children.

So the security that's required to manage a small school through the county council market is very different to managing a university network. And that's also different to a global university trying to operate in different markets you see that can operate globally.

And the students, they can be diverse, different countries, different cultures, different devices, different technologies. All have to be coped with and provisioned with different systems.

So you've got everything from basic email access, right the way through to database management. But you've also got manufacturing systems, you've got research systems, you've got IP protection, all of which has to be wrapped up in compliance, GDPR in education.

Those networks are public and the facilities are paying for it in most countries now. So it's an enterprise in its own right, but a lot of them are incredibly complicated beasts and require very specific solutions. The generics work at the top level for the top sort of layer of security is not as simple and as it moves forward, the 'one-stop-shop' or 'one-size-fits-all' dœsn't really work. They have to build different layers.

Andrew: So, given the size and nature of networks in education, what advice could you give to the facilitators and IT security to best avoid any threats and security breaches?

Adrian: It's got to start with budget. Budget and planning. How do you get it? What plan do you put in place to get it? How thorough do you think that through? Because one size dœsn't fit all.

You've got such diverse user communities. In terms of local government, for instance, funding for county council is for everybody. It has to work for the guy who picks up your rubbish in the bins, a forestry worker, the staff in the county council and also the schools because they can draw those. Whereas a university has a different route to get the money.

The planning is essential. The user community is not a corporation. They are very much individuals and they're not IT literate at the gate so will not comply with the company rules in the same way council workers would.

Because, help desk management don't have the staff and the manpower to deal with after-the-fact issues. So you need a fairly automated autonomous system, but you need to have something which is flexible enough for you to build your solution within the corporate environment.

I would say the fundamental thing though is definitely planning and allocation of money. I think it was JISC that put out a report very recently, a survey they did into funding, saying there was a marginal increase. In other words, the budget's not going to go up massively despite the funding levels, across from third parties or private funding and the international students.

At the end of the day, it's a very tight budget system with a very big demand on it and very few people involved. So the more you automate it and the more you plan for that budget, the bigger benefit there's going to be.

As with any enterprise network security system, you have to make the plan, test the plan, implement, and then you'll get the result you wanted. If you rush it through and try to make a quick decision on it without all the facts it can really kill you long term as the devil is in the detail.

Andrew: It is generally accepted that there's a massive shortage of IT security skills at the moment. Specifically, how do universities and other educational facilities go about addressing that?

Adrian: It's a tough one. In fact, actually I'd sort of narrow it down again. While IT skills are hard, networking skills are, I think, even harder. Then cybersecurity skills go beyond both those.

I mean, often in education, there's no process to keep up with current technologies. The problem is they move so fast. By the time you're qualified, you're four years out of date. So, you've got to find somebody who's already in that marketplace moving it forward.

There is a lot of work trying to get people involved, it's a full-time job to bring people in to do that. But they're few and far between. And they're spread very thin.

The best place is to either self-educate, to bring yourself up to speed. To go out and find educational forums online, talk to your peers, talk to your colleagues, talk to other universities, or people on the same levels, because, again there are different requirements for different sectors.

The other option is the suppliers, if they're a good supplier. If they want to sell you something, you walk away. If they want to talk to you about it and address the issue you have and skill you up and to help and train you, that's part of the argument. That's part of the solution because you will get the better knowledge. And then you'll start asking those questions, well, what about this? How does that work? What issues are going to be addressed by that?

That's what really needs to happen. I think it'll catch up with itself. Assuming we can get the budgets involved in education to bring those people forward.

And if you look at universities, there are courses and that way you're specifically going on the government's initiative, you know with the Cybersecurity centre down at GCHQ and the suppliers themselves, they're thinking more about how we can protect all aspects of our community and particularly education and children. So, I think further education has got a specific set of needs and schools. It's a different, it's a harder problem. There is no dedicated IT resource, they have to refer back. But there's now such thing as self-learning. Be aware of it, that's probably the key thing but knowledge is power.

Andrew: Obviously, a lack of funding and stretched resources present a challenge. Given the sprawling nature of the IT networks in the education sector, how can we go about securing these devices?

Adrian: Well, it's not just the device, it's the user. But let's take the devices issue. Typically, in the old days, there was a mainframe in the university. If you want to get in, you type your username and password and it would let you in, probably a WAN or a local Cray Mainframe. And that was it. That was the system. Now if you look at my daughters, they turn up to university with a laptop, phone, iPad, mobile devices, tablets. They've got multiple devices that they all want to have access to the same thing in theory. But they're all (as far as an IT security professional is concerned) foreign devices.

The only common denominator is the person. Can I authenticate that you are you using that device? Every system they use is different, but all students now would expect to have a level of access to a large range of applications. E-learning is the basis. You have the assessment system, the review system, the coaching and mentoring system. The exams themselves are virtually all online and the systems that support the student.

Office, Excel, PowerPoint, the basic office suites plus all of the specific applications. If they study Media Statistics, Products, Design, all those applications are online and available for them to use on their devices in different ways.

Controlling access is the critical one and the only way you can do that is with authentication at some level. And because there's a broad range of devices and a broad range of applications, you need multifactor authentication. That's both factorial in the sense of the device control, right time, right place, right IP, right location, but also the person. Using fingerprint recognition or PINs. Not a static PIN and dynamic PIN. A proper 2FA or multifactor authentication.

Those things combined can secure what is now a vast array of applications that are just as different as students. Whether it be a school, a kid who wants to look on her iPad, right the way through to a further education [student] learning online for, you know, an architecture degree. Google is the place you go. You go to the library to use Google. That's what's changed.

Andrew: So now we've secured the devices, how do the campuses go about securing their systems?

Adrian: That's an even bigger issue. If you know the people that are coming in and the problem is the diversity. Let's take the university and not talk so much about our schools, but let's take a bigger education facility. They have such a vast array of application needs and security needs.

You've got everything from perimeter security, physical security: doors, buildings, parking, access control systems, right the way through to POS systems, tills, they take an awful lot of money.

Take student bars - is the video camera system in there providing a feed that's being matched up with the Epos data that's then also matching up the person logged in on the till at 2 o'clock this afternoon? And so they're the one taking the money right the way through to cybersecurity resilience on student applications.

Now that also might be a manufacturing system, because they might build satellites and there's a development engineering team with core IP in there. They might be, an engineering technical university.

There's all sorts of different systems. So I think it's verging on cruel or unfair to expect an IT department in an education sector to suddenly start becoming experts in all these fields. Even with self-learning and education.

You have to separate the systems. You have to try and get best practice in those systems discreetly and then look for solutions that bring them together in a way that's controllable. The biggest challenge is, we pull them all together and then they don't work or they don't do quite what you think they were going to do and you're back to the same thing.

Flexibility dœsn't do what it says on the tin. Can I prove that it dœs what it says on the tin before I buy it? Is it cost effective? Because there are amazing solutions out there, but they cost so much money. Identity Management, which is IDAS or the cheap version Identity as A Service. Yes it's a fantastic thing to have. But you need to have the roadmap and the journey and the process, and the buy-in from everybody to go and implement it. It's a lot of money. It's a lot of time and it's a long process.

Continued >>

Adrian: What do you do between now and then? I tell you what, when a student turns up at a university with a laptop and says, "I want to connect to get office 365". You say, no problem at all. Here's your username and your email address from the uni. There is your password. By the way, you're going to install this app and that automatically comes in because we do mobile device management, another self-help. And that gives you multifactor authentication. So, every time you log in, it's a different set of criteria for you to log into the system rather than just the username and password to see you through for 4 years.

That's not a robust security solution.

So there are some things you can put in place that are relatively low cost, and some things that take a lot more thinking about and a lot more time. You've got to have a strategy for all of them and run them and then plan them and put them into place.

Andrew: So, we can have all the best practices in the world. However, students/users have a massive part to play in this. How do we make sure they know what their responsibilities are?

Adrian: I think there's a balance between control and education. Some policy management has to be enforced. Although it's very difficult to do when you've got a student community and members of staff who bring their own equipment. It's not yours to control as it is in a corporate environment, like we talked about before.

All you can do is to mitigate the user errors. To train them on what's available, what systems will and won't work for them, what things they should and shouldn't do. 'Don't click on these links. Don't do those things. Be aware of social media. Here are some rules' etc. and then put structures in place, whether that be user behaviour tracking, whether that be control of actual physical access to networks or services and sites, web application, firewalling, identity management in terms of the person and also authentication.

But then beyond that is all the other things that you have access to as a student that you expect to see because you're so used to having everything open to you on all your devices.

There is no way you can impose a corporate device management policy by saying we're going to install this, this, and this on your personal phone, without you agreeing to it. So it's kind of an education process and also an enforcement process.

The problem with both scenarios is they cost money. Both in terms of education, you have to go and produce the information, share it in the right way via the internet or at enrolment and make that a regular part of the syllabus for everybody, including staff.

Or, you go with the enforcement group, and set out what users can and can't do. And you can do that to a certain extent, but if you push too hard, they'll just ignore it.

That's just the nature of the people. So you need to have some form of corporate controls or should we say or corporate standards, but you cannot enforce them in the same way. Because it's not corporate. It's an education establishment.

It's all about collaboration. Know what you can do and what you can't do. Be aware of what's wrong and what's right and then you can make an informed decision and if your informed decision is incorrect, make sure that the IT department's got a way to stop you from doing it at the very extremes if it's that dangerous in that particular area or particular site or whatever, or a link.

Invariably it comes down to getting people's buy-in to do it this way, in the best way. Rather than forcing it on somebody.

Andrew: I think we've covered some really interesting topics today. What would you say is the most significant or biggest takeaway from it?

Adrian: I suppose there are two things. One, in general terms, is for security. It's a huge problem, so you have to break it up into manageable pieces, manageable projects, and you've got to budget for them and plan them before you implement them.

In terms of authentication, so our space: do authentication first. There's a myriad of choices out there, and you can work through which ones are sensible for you. Do your authentication before you go straight into identity management. As soon as you go into identity management there's big budgets, big stakeholders, lots of issues, lots of rollout. Long term stuff. It requires a massive amount of cost, infrastructure, time and people.

So do the quick wins while you can and secure, and then move on through your planning cycle.

For more information, get in touch or visit swivelsecure.com.

FAQs

Education Cybersecurity

At Swivel Secure we work with many education facilities to help prevent unauthorised access to their virtual learning environment, with our intelligent multi-factor authentication (MFA) solution – AuthControl Sentry®. AuthControl Sentry® authenticates students and staff using a wide range of authentication factors. Providing advanced functionality such as single sign-on and risk-based authentication as standard, AuthControl Sentry® is one of the most cost-effective MFA solutions for Education facilities.

Can Swivel Secure integrate with Computing at Schools?

Yes, Swivel Secure's AuthControl Sentry® can integrate with Computing for Schools or CAS. Most of our customers are members of CAS, with an increased focus on Computing in schools. AuthControl Sentry® is utilised by CAS members as a multi-factor authentication solution because of its risk-based authentication functionality.

Can Swivel Secure integrate with Moodle?

Yes. Moodle is a free and open-source learning management system written in PHP – Hypertext Preprocessor, which is a general-purpose programming language Swivel Secure's AuthControl Sentry® can integrate with Moodle and therefore help education facilities from protecting unauthorised access to their virtual learning environment.

Can AuthControl Sentry® protect Office 365?

AuthControl Sentry®, the multi-factor authentication platform from Swivel Secure protects a wide range of applications including Office 365 and OWA Outlook Web App. The platform provides two-factor authentication, risk-based authentication, and single sign-on functionality, AuthControl Sentry® can integrate with both Microsoft ADFS 3 and ADFS 4.

Can AuthControl Sentry® authenticate students and staff when they are off campus?

Both students and staff regularly access their research, timetables, syllabus content and marked assignments when they are off campus, making it difficult to secure applications such as virtual learning environments. Implementing risk-based authentication (RBA) with AuthControl Sentry®, delivers intelligent authentication by optimising security, based on the user, the device and the application. Utilising RBA provides reassurance that even if students are accessing their virtual learning environment off-campus, they will be requested to provide the appropriate level of authentication based on their particular scenario i.e. if they are accessing virtual learning environment from a coffee shop they would need to provide stronger authentication to successfully authenticate access.

How easy is it to provision users?

One of the benefits of implementing AuthControl Sentry® is the self-service User Portal, making it extremely easy for users to be self sufficient, saving on administrator support overheads. Swivel Secure's User Portal is designed to deliver greater efficiency for users to execute basic requirements including changing their PIN, resetting their PIN, mobile app provisioning, and hardware token resynchronisation.

Is the AuthControl Sentry® platform easy to use?

Yes, with one of the widest ranges of authentication factors available, AuthControl Sentry® is extremely easy to use. One of the easiest factors to use is the OneTouch PUSH notification via the mobile app. Users wishing to authenticate, simply receive a PUSH notification via the mobile app. They then select YES or NO when asked if they'd like to continue with authentication.

What authentication factors can students and staff use?

Authentication methods include: Fingerprint, Mobile App, SMS, Email, Hardware Tokens, and Image-based Authenticators (TURing/ PINpad®). Hardware tokens are still supported, but most of our customers opt for authenticating using the mobile app, SMS or PINpad®. Both short messaging service (SMS) and the mobile app can be used, offering optional authentication methods including a OneTouch PUSH authentication, allowing users to simply accept or reject the authentication. For those that prefer not to use mobile devices on campus, users can easily authentication using Voice. Providing auditory functionality for PUSH and one-time code (OTC), Voice enables users to authenticate when the use of mobile or a physical token may not be permitted. By calling the user, AuthControl Voice vocalises either a one-time code (OTC) or a PUSH notification (YES or NO) to authenticate access to applications. The OTC delivered vocally over the telephone is then typed into the window upon request.

Protecting identities with intelligent authentication

USA & APAC Office
Swivel Secure, Inc.
1340 Reynolds Ave. #116-285
Irvine, CA 92614
E: **usa@swivelsecure.com**
T: **+1 949 480 3626** (Pacific Time)
Toll Free: **866.963.AUTH** (2884)

UK & Ireland (North)
Swivel Secure Ltd
1200 Century Way
Thorpe Park
Leeds
LS15 8ZA
E: **hq@swivelsecure.com**
HQ T: **+44 (0)1134 860 123**
Support T: **+4 (0)1134 860 111**

EMEA Offices
Portugal
Estrada de Alfragide,
N67 Lote H, Piso 0 (Alfrapark)
2614-519 Amadora
Alfragide, Portugal
E: **portugal@swivelsecure.com**
T: **+351 215 851 487**

Spain
Calle Punto Mobi 4,
28805 Alcala de Henares,
Madrid, Spain
E: **espana@swivelsecure.com**
T: **+34 911 571 103**

swivelsecure

www.swivelsecure.com