Improving Cyber and Information Security

Andrew Williams
Online Safety and Information Security Consultant
South West Grid for Learning

SWGfL
Safe. Secure. Online

ITPro. Business Cloud Hardware Infrastructure Security Software Technology Resou

15 schools in Nottinghamshire crippled by cyber attack

The Nova Education Trust is unable to access its IT systems to conduct remote lessons

by Bobby Hellard 4 Mar 2021

Schools across Nottinghamshire have had to shut down their IT networks after a central trust that manages their systems was hit by a cyber attack.

All 15 secondary schools that are part of the Nova Education Trust are currently unable to access emails or their websites, and are still unable to conduct lessons remotely.

- Hackers hold Newcastle Uni student data to ransom
- Exams cancelled after Northumbria University cyber attack
- What is ransomware?

The trust has alerted the National Cyber Security Centre (NCSC) which is currently working with its central IT team to resolve the matter. The incident has also been reported to the Department of Education (DfE) and the Information Commissioner's Office (ICO).

The attack was first discovered on Wednesday morning, prompting the trust to shutdown every one of its systems as a precaution. It added that its central IT team is still investigating the potential impact of the attack

Each school associated with the trust has also been advised to shut their systems down while the

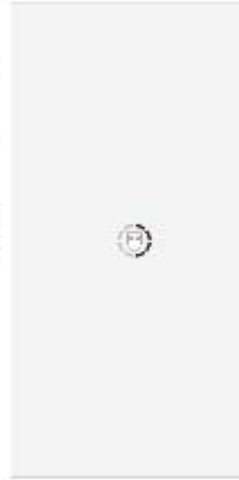
Search ...

Fears as 'thousands' of cyber attacks launched against British ...rsities

W...

We...

20...



Matt Hancock UK

ISLE OF WIGHT SCHOOLS NEED DATA AFTER CYBER ATTACK

News Home | More from Isle of Wight News

Tuesday, August 24th, 2021 10:28am

By Oliver Dyer @olidyer

Parents of students at Isle of Wight schools hit by ransomware attacks are being asked to get in touch after vital data was lost.

As Isle of Wight Radio first reported, cyber attacks left school websites inaccessible and data 'frozen' earlier this month.

Staff at Medina and Carisbrooke College, as well as the Island VI Form, were affected, as were Barton Primary, Hunnyhill Primary and Lanesend Primary.

As such, affected schools are carrying out a data collection exercise. This would usually happen at the start

IE NEWS FEATURES COMMENT WEBINARS PODCAST EVENT REPLAY DIRECTORY PROFILE LOGIN

Independent Education Today | For leaders of independent schools

News

The growing importance of cybersecurity in schools

Sponsored: iSAMS explores the most effective ways schools can protect themselves against cyber scammers

Contributor

In 2020, the UK's Department for Digital, Culture, Media and Sport conducted a Cyber Security Breaches Survey with a section focused specifically on the education sector. Its findings made for perturbing reading. The results of the survey showed that 41% of primary schools, 76% of secondary schools and 80% of further education institutions had identified at least one cyber-attack or security breach in the previous 12 months.

Hackers and cybercriminals appear to be increasingly turning away from larger organisations in favour of targeting smaller institutions – seen as low hanging fruit – that may be less well equipped to deal with a scam or hacking attempt. The fallout from a security breach can have devastating consequences for schools.

Previous attacks have resulted in significant financial losses, sensitive data on students, parents and staff being lost or published online and have even forced temporary school closures. With schools firmly in the crosshairs of cybercriminals, the importance of a secure digital infrastructure has never been greater.

One of the most effective ways to protect against cyber scammers is training staff to spot phishing attacks and malicious downloads, and implementing safety checks such as 2FA (two-factor authentication) for all school systems.

Hackers and cybercriminals appear to be increasingly turning away from larger organisations in favour of targeting smaller institutions

Cybercriminals can embed malware in email attachments, which if downloaded can spread through a school's network

fe news.co.uk

Sign up for em... all the latest su...

HOME PUBLISH SEARCH FEATURES VIDEO & PODCASTS SECTOR NEWS

93% increase in cyberattacks targeting the UK's education sector

fe news by Check Point Research Published: 23 August 2021 Hits: 1255 Vote 5 Rate

As back-to-school begins, Check Point Research (@_CPResearch_) found the education sector to have the highest volume of cyber attacks for the month of July. Cyber criminals are seeking to capitalize on the short-notice shift back to remote learning driven by the Delta variant, by targeting people of schools, universities and research centers who log-in from home using their personal devices.

- Global education sector saw a 29% increase in cyber attacks, and an average of 1,739 attacks a week, in July, compared to first half of 2021
- Top 5 most attacked countries were India, Italy, Israel, Australia and Turkey
- UK/Ireland/Isle-of-Man region experienced a 142% increase in weekly cyber attacks targeting the education sector; East Asia region marked a 79% increase

93% increase in cyberattacks targeting the UK's education sector

Check Point Research (CPR) sees an increase in cyberattacks against the global education sector, as back-to-school season gets underway. During the month of July, the education sector experienced the highest volume of cyber attacks compared to other industry sectors that CPR tracks, with an average of 1,739 cyber attacks documented per organization each week, marking a 29% increase from the first half of

SKILLS WORLD LIVE

Why we are contacting you?

The Department for Education and the National Cyber Security Centre (NCSC) has been made aware of an increasing number of cyber-attacks involving ransomware infection affecting the education sector at this time. The purpose of this letter is to make you aware of the threat and provide high-level information and advice to support your ongoing cyber security preparedness and mitigation work.

In all cases the NCSC has been working with the department and the affected providers to contain and support post-incident outcomes. However, these attacks and incidents have had a significant impact on the affected education provider's ability to operate effectively and deliver services.

These incidents appear to be financially driven but opportunistic, taking advantage of system weaknesses such as unpatched software, poor authentication systems or the susceptibility of users to misdirection.

Whilst I would urge you to ensure that your systems, processes and awareness training are up to date, I also want to make you aware of the steps you should take if your educational setting is affected.

teiss News CISOs Threats Culture & Education Opinion Events Video teissTalk White Papers

Harris Federation suffers a ransomware attack, shuts down email and telephone systems

March 31, 2021

Education charity Harris Federation has become the fourth multi-academy trust to have suffered a ransomware attack since late February. The ransomware attack has forced the charity to shut down IT systems, and temprarily disable its email system and switchboard services.

The Harris Federation, which now runs fifty primary and secondary academies in London and Essex with more than 36,000 pupils enrolled, announced on Monday that it suffered a ransomware attack last Saturday that enabled hackers to access its IT systems and encrypt their contents. The charity is presently working with cyber security experts to investigate the attack and restore all affected systems.

In a press release, Harris Federation said that after discovering the ransomware attack, it disabled its email system used by more than 40,000 students, as well as its telephone systems and switchboard services as a precaution.

Home Information for... Advice & guidance Education & skills Products & services News, blogs, events...

Home » Alert: Further ransomware attacks on the UK education sector by cyber criminals

NEWS

Alert: Further ransomware attacks on the UK education sector by cyber criminals

The NCSC is responding to further ransomware attacks on the education sector by cyber criminals.

PUBLISHED
4 June 2021

NEWS TYPE
Alert

WRITTEN FOR
Large organisations
Small & medium sized organisations
Cyber security professionals
Public sector

Download / Print Article PDF

Share

Was this article helpful?
Yes No

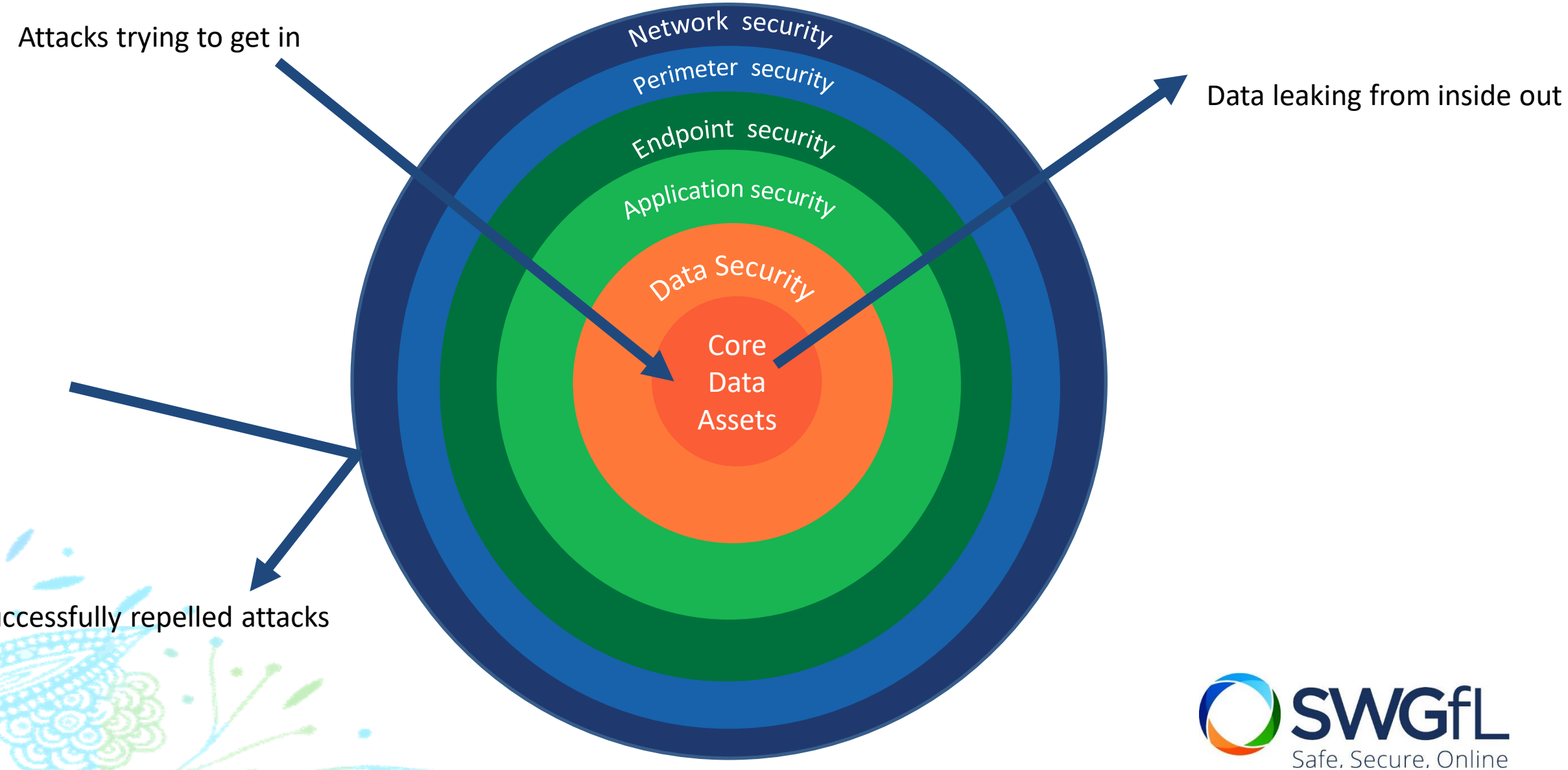
IN THIS ALERT
1. Introduction

Safe, Secure, Online

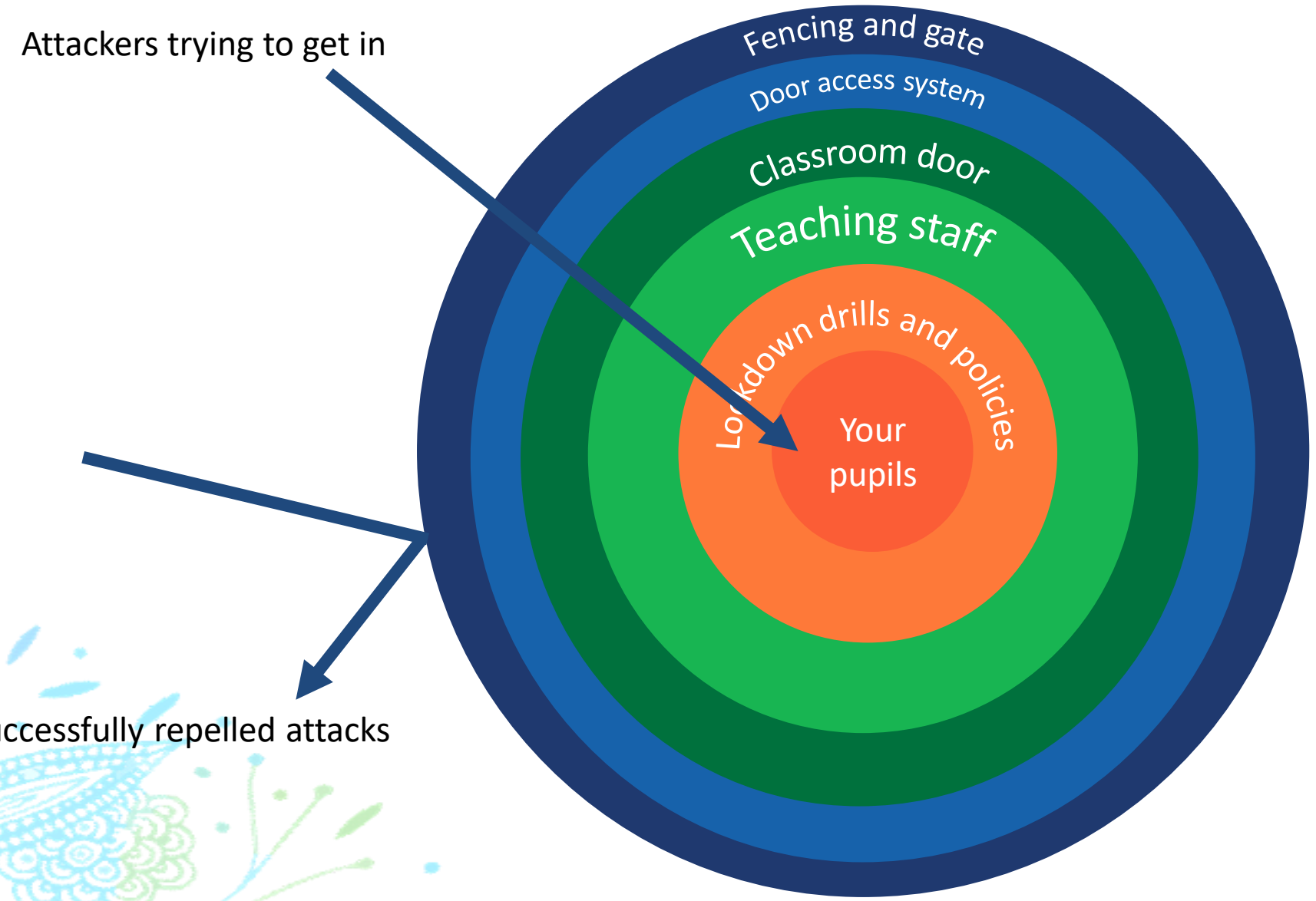
Safeguarding implications

- Can you operate your establishment without access to:
  - Parent contact details
  - Pupil records
  - Contact details for third parties
  - Telephone systems
  - Email
  - The internet
  - CCTV
  - File servers
  - Door/gate access control…?
- What would be the implications for you, your staff and your pupils if personal information was leaked onto the dark web?

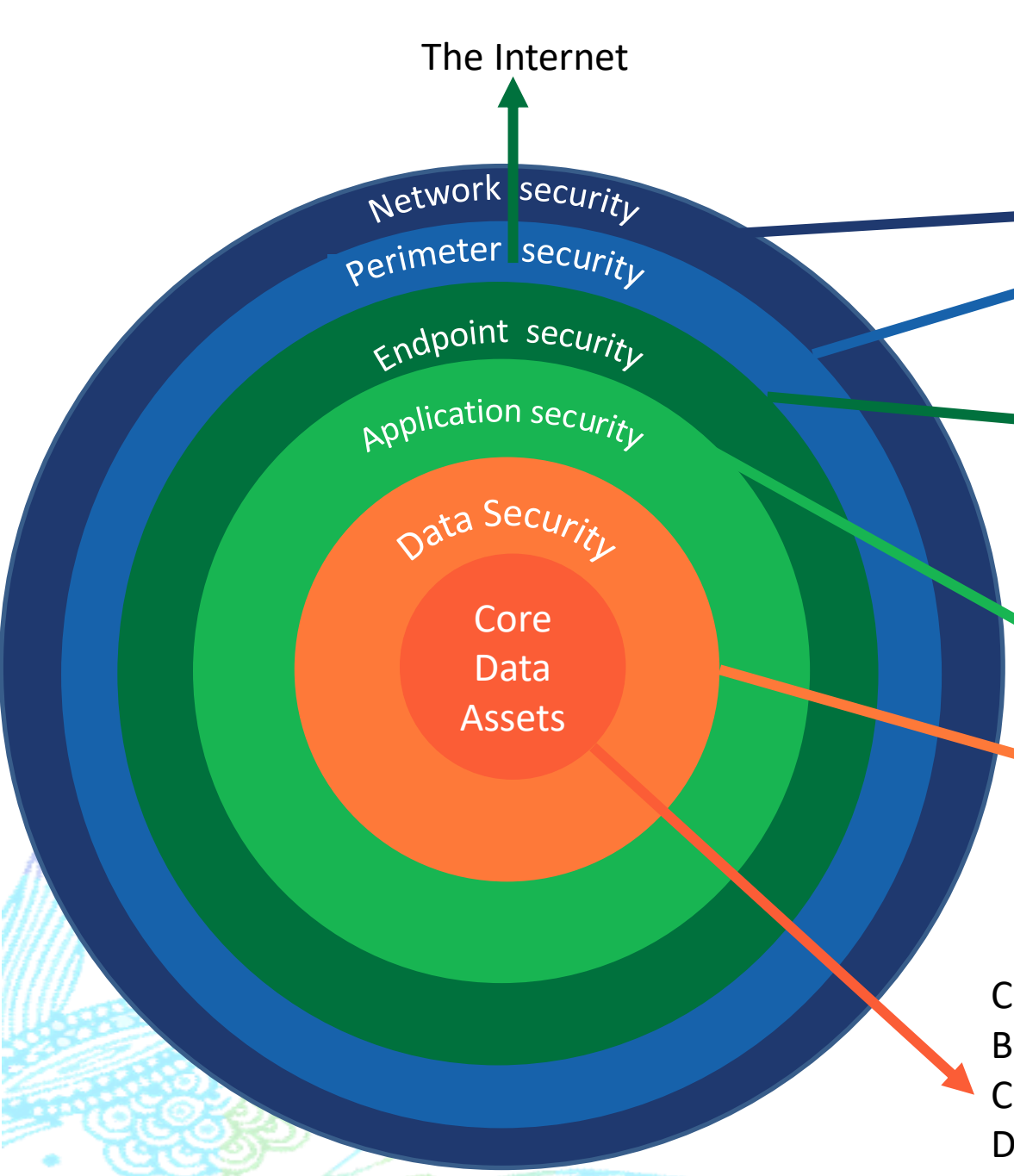
SWGfL
Safe. Secure. Online



SWGfL
Safe. Secure. Online



SWGfL
Safe. Secure. Online



Firewall
Servers/switches
Routers
ISP
Filters
Monitoring
Intrusion detection systems

Anti-virus
Anti-malware
Ransomware protection
Anti-exploit
Fileless attack prevention
Asset management
MDM
Device firewall

Software patching
Automatic updates
Logging systems
Access controls
Password security

Policies
Record of Processing Activities
Maps of critical data
Data access controls
Retention and disposal

Critical data identified and protected
Backed up
CIA
Data Loss Prevention
Security Information and Event Management (SIEM)

Underpinned by staff training at all levels

SWGfL
Safe. Secure. Online

Insider threats

Lepide Home | Data Security & Compliance Blog

College Campuses are a Breeding Ground for Insider Threats

by Jason Coggins Updated On - 06.18.2020 Data Security

A recently published report by Infoblox Inc. discovered that over 80% of IT professionals working at higher learning institutions find securing campus networks to be more of a challenge every year.

The report (Defending Networks at Higher Learning Institutions – Heroes Needed) gathered information from more than 600 students and employees at educational organizations across the

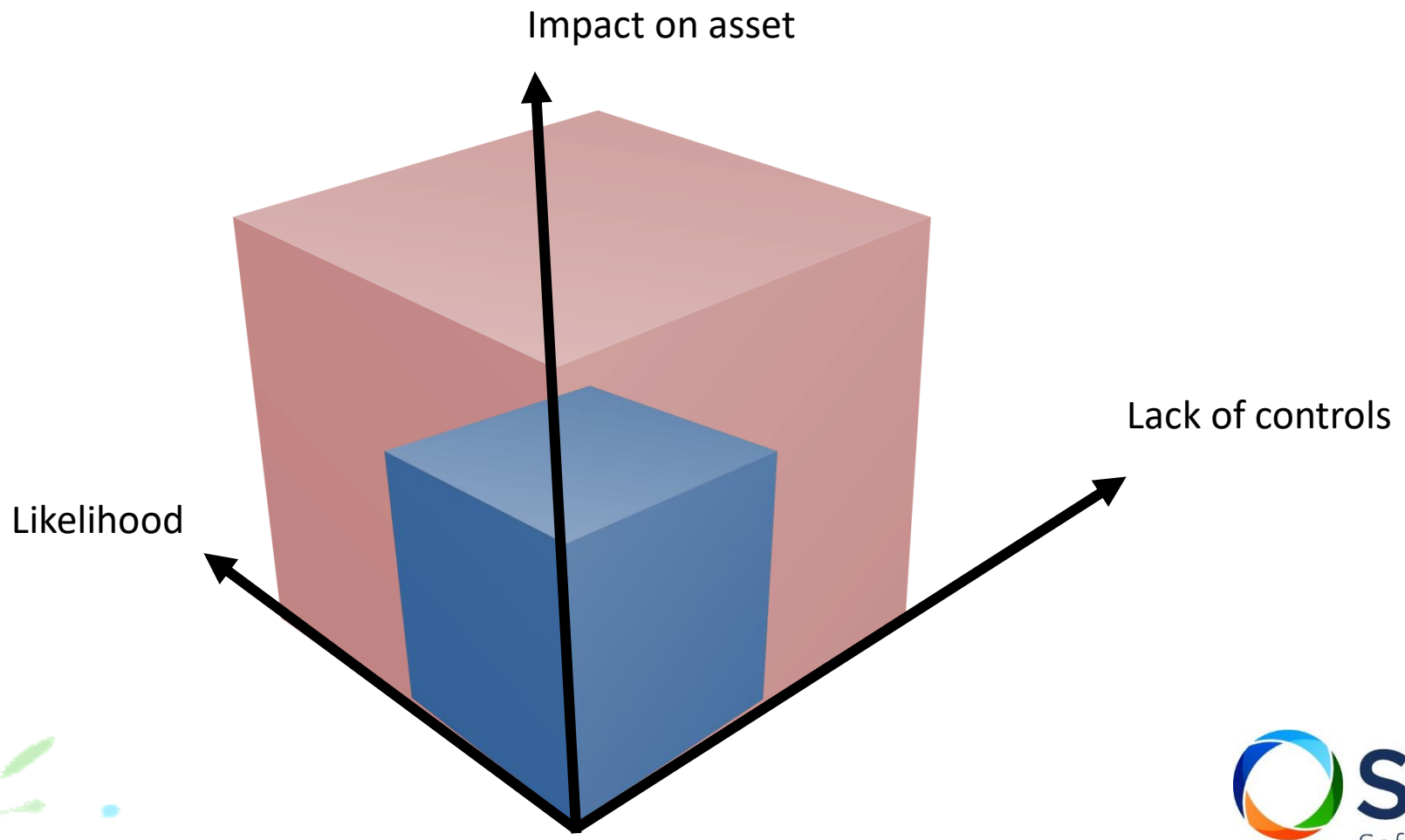
- Staff need access
- Students try to get access
- Unauthorised Data Sharing

Prevention:

- Training
- Monitoring
- DLP
- Audit and identify core data

SWGfL
Safe. Secure. Online

Risk mitigation



SWGfL
Safe. Secure. Online

Baby photo created by jcomp - www.freepik.com

Kids photo created by freepik - www.freepik.com

Tree photo created by valdavitaly - www.freepik.com

GfL

re, Online

Auditing

Data

Where is it?
Is it core data?
Who has access to it?
Does it need securing?

Devices

Where are they?
What do they do or store?
Who has access to it?
Does it need securing?

Users

Who needs access to what?
Defining different roles?
Have they had appropriate training?
Do they understand their obligations?

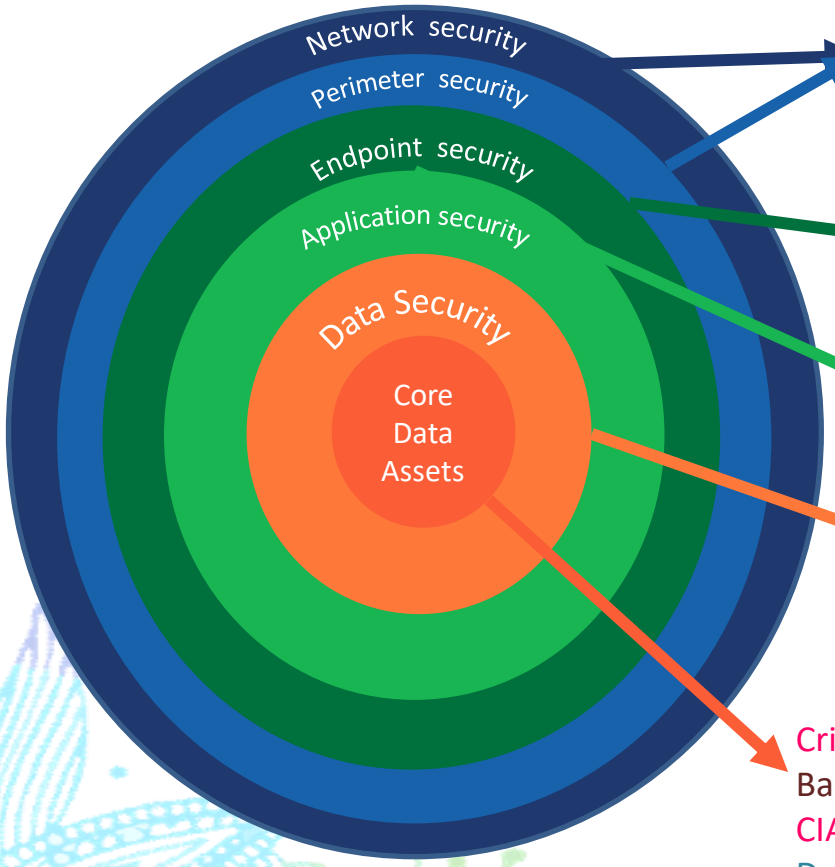
Breaches

Is there a plan?
Does the plan work?
Does everyone know how to initiate it?
Does it include out-of-hours?
Is a copy stored off-site?

4 “D’s”:
Define, Do, Document, Deal

SWGfL
Safe. Secure. Online

Protection against attack



Firewall
Servers/switches
Routers
ISP
Filters
Monitoring
Intrusion detection systems

Anti-virus
Anti-malware
Ransomware protection
Anti-exploit
Fileless attack prevention
Asset management
MDM
Device firewall

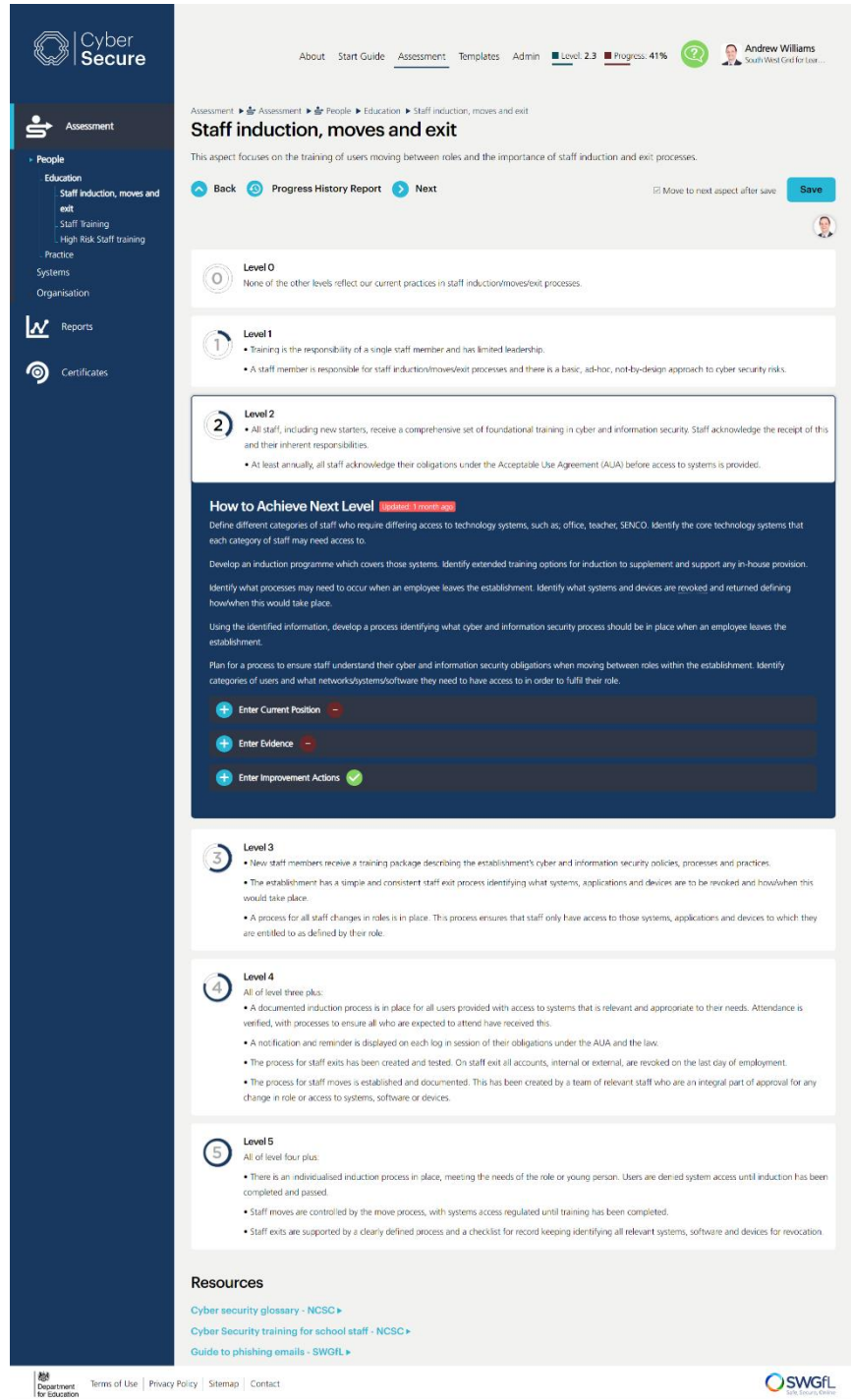
Software patching
Automatic updates
Logging systems
Access controls
Password security

Policies
Record of Processing Activities
Maps of critical data
Data access controls
Retention and disposal

Critical data identified and protected
Backed up
CIA
Data Loss Prevention
Security Information and Event Management (SIEM)

Software
Hardware
Software/Hardware
Systems – Policy/People

SWGfL
Safe. Secure. Online


Cyber Secure
About
Start Guide
Assessment
Templates
Admin
Level: 2.3
Progress: 41%
Andrew Williams
Assessment
People
Education
Staff induction, moves and exit
Staff Training
High Risk Staff training
Practice
Systems
Organisation
Reports
Certificates
Assessment ▸ Assessment ▸ People ▸ Education ▸ Staff induction, moves and exit
Staff induction, moves and exit
This aspect focuses on the training of users moving between roles and the importance of staff induction and exit processes.
Back
Progress History Report
Next
Move to next aspect after save
Save
Level 0
None of the other levels reflect our current practices in staff induction/moves/exit processes.
Level 1
• Training is the responsibility of a single staff member and has limited leadership.
• A staff member is responsible for staff induction/moves/exit processes and there is a basic, ad-hoc, not-by-design approach to cyber security risks.
Level 2
• All staff, including new starters, receive a comprehensive set of foundational training in cyber and information security. Staff acknowledge the receipt of this and their inherent responsibilities.
• At least annually, all staff acknowledge their obligations under the Acceptable Use Agreement (AUA) before access to systems is provided.
How to Achieve Next Level
Updated: 1 month ago
Define different categories of staff who require differing access to technology systems, such as; office, teacher, SENCO. Identify the core technology systems that each category of staff may need access to.
Develop an induction programme which covers those systems. Identify extended training options for induction to supplement and support any in-house provision.
Identify what processes may need to occur when an employee leaves the establishment. Identify what systems and devices are revoked and returned defining how/when this would take place.
Using the identified information, develop a process identifying what cyber and information security process should be in place when an employee leaves the establishment.
Plan for a process to ensure staff understand their cyber and information security obligations when moving between roles within the establishment. Identify categories of users and what networks/systems/software they need to have access to in order to fulfil their role.
Enter Current Position
Enter Evidence
Enter Improvement Actions
Level 3
• New staff members receive a training package describing the establishment's cyber and information security policies, processes and practices.
• The establishment has a simple and consistent staff exit process identifying what systems, applications and devices are to be revoked and how/when this would take place.
• A process for all staff changes in roles is in place. This process ensures that staff only have access to those systems, applications and devices to which they are entitled to as defined by their role.
Level 4
All of level three plus:
• A documented induction process is in place for all users provided with access to systems that is relevant and appropriate to their needs. Attendance is verified, with processes to ensure all who are expected to attend have received this.
• A notification and reminder is displayed on each log in session of their obligations under the AUA and the law.
• The process for staff exits has been created and tested. On staff exit all accounts, internal or external, are revoked on the last day of employment.
• The process for staff moves is established and documented. This has been created by a team of relevant staff who are an integral part of approval for any change in role or access to systems, software or devices.
Level 5
All of level four plus:
• There is an individualised induction process in place, meeting the needs of the role or young person. Users are denied system access until induction has been completed and passed.
• Staff moves are controlled by the move process, with systems access regulated until training has been completed.
• Staff exits are supported by a clearly defined process and a checklist for record keeping identifying all relevant systems, software and devices for revocation.
Resources
Cyber security glossary - NCSC ▸
Cyber Security training for school staff - NCSC ▸
Guide to phishing emails - SWGfL ▸
Department for Education
Terms of Use
Privacy Policy
Sitemap
Contact
SWGfL

gfL Online

National Cyber Security Centre

CyberFirst

We're developing the UK's next generation of cyber professionals through our student bursaries, courses for 11-17 year olds and competitions.

Learn more about CyberFirst

CyberSprinters

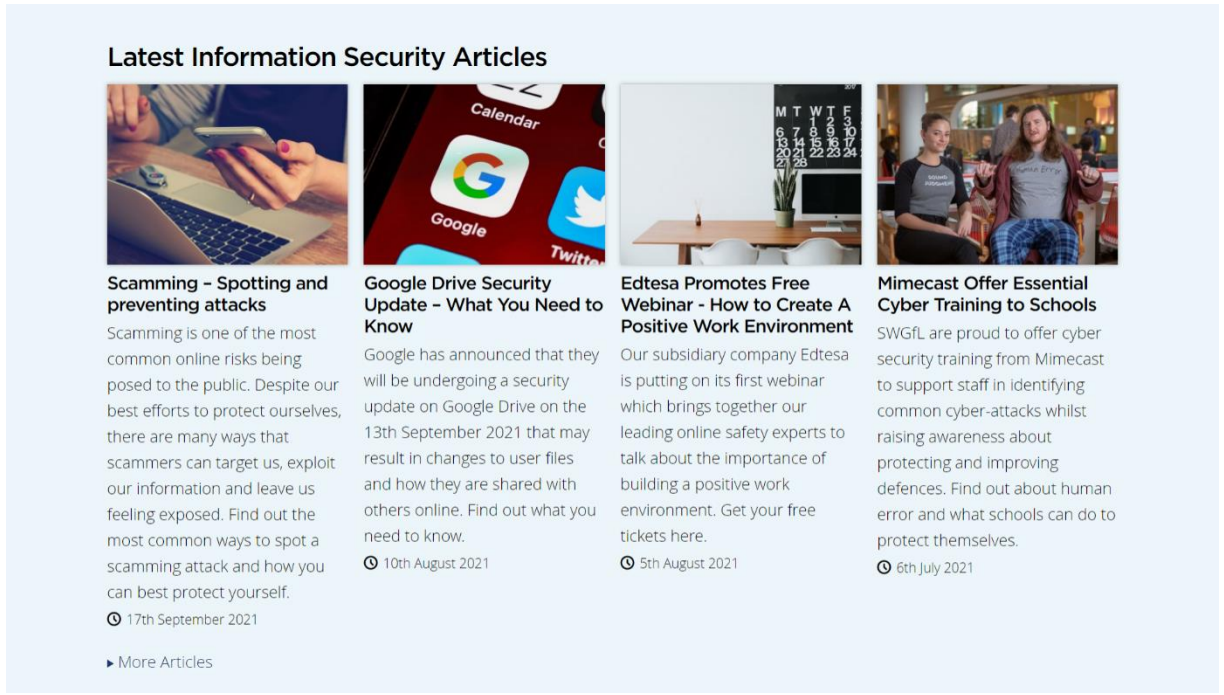
Exciting new interactive online security resources for 7-11 year olds.

Game and activities

SWGfL
Safe. Secure. Online

https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools

SWGfL
Safe, Secure, Online



https://swgfl.org.uk/security/

Thank You

Please:
Visit OnlineSafetyLive.com – free online safety training for all CSS by SWGfL - Free cyber secure schools conference save the date **13th October!**
Look out for CyberSecure from the DfE

Andrew Williams

swgfl.org.uk
enquiries@swgfl.org.uk
@wenglishgeek

SWGfL
Safe. Secure. Online