



Schools Under Attack: Why Education is a Target



Today`s Schedule

- Education Threat Landscape
- Why Schools?
- Seasonality
- Awareness: The Essential First Step
- Case Studies
- EdSecure from Moore ClearComm
- Questions

Guest Panel:

Clare Moore
Head of Compliance



Paras Shah
Cyber Security Consultant



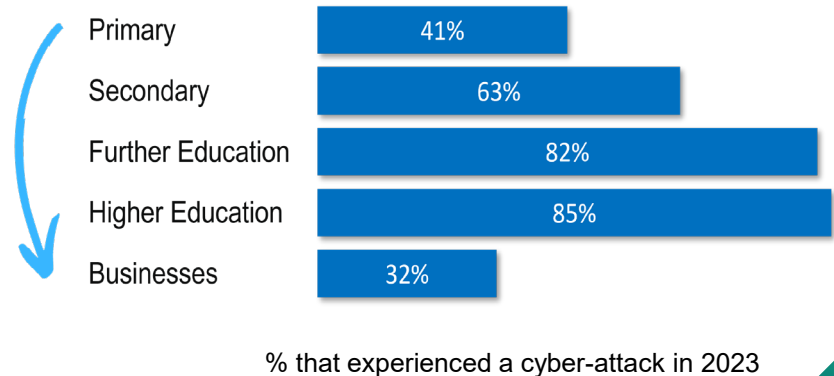


MOORE ClearComm

Threat Landscape

Latest Data from UK Gov & NCSC (2023 Report)


- All types of education institutions are more likely to identify breaches or attacks than the average UK business
- Education is now a more likely deliberate target for cyber criminals, than commercial businesses
- Primary schools are the least likely (within education) to experience cyber attacks
- Further and higher education institutions are the most likely
- Primary schools are still more likely to be attacked than other commercial organisations



Common Threats

Commonly targeted data in schools / colleges / universities:

- ✓ Financial systems
- ✓ Personal identifiable data
- ✓ Intellectual property
- ✓ Student coursework
- ✓ Student personal data
- ✓ Cloud services
- ✓ MIS/SIMS database



“Spending money on cyber security is rarely politically popular in schools – and they often don’t know where to spend the money either.”

Brett Callow
(Cyber Threat Analyst)

Common Threats

Phishing & Social Engineering

Fraudulent attempts to obtain sensitive information or prompt action. Most common type of attack across all educational institutions

Viruses, Spyware, or Malware

Software designed to damage, disrupt, or gain unauthorised access to systems. This is a significant threat, especially in higher education institutions

Denial of Service (DoS) Attack

Overwhelming a network/service with traffic to make it unavailable to users. More common in further and higher education institutions

Common Threats

Unauthorised Access

Accessing files or networks without permission by students, staff, or external attackers. Notable risk in secondary and higher education institutions

Ransomware

Malicious software that locks/encrypts data, ransom demand to unlock data. Affects all educational sectors to varying degrees

Business Email Compromise (BEC)

Gaining access to a business email account and imitating the owner's identity to defraud. Increasingly common across all sectors, including education



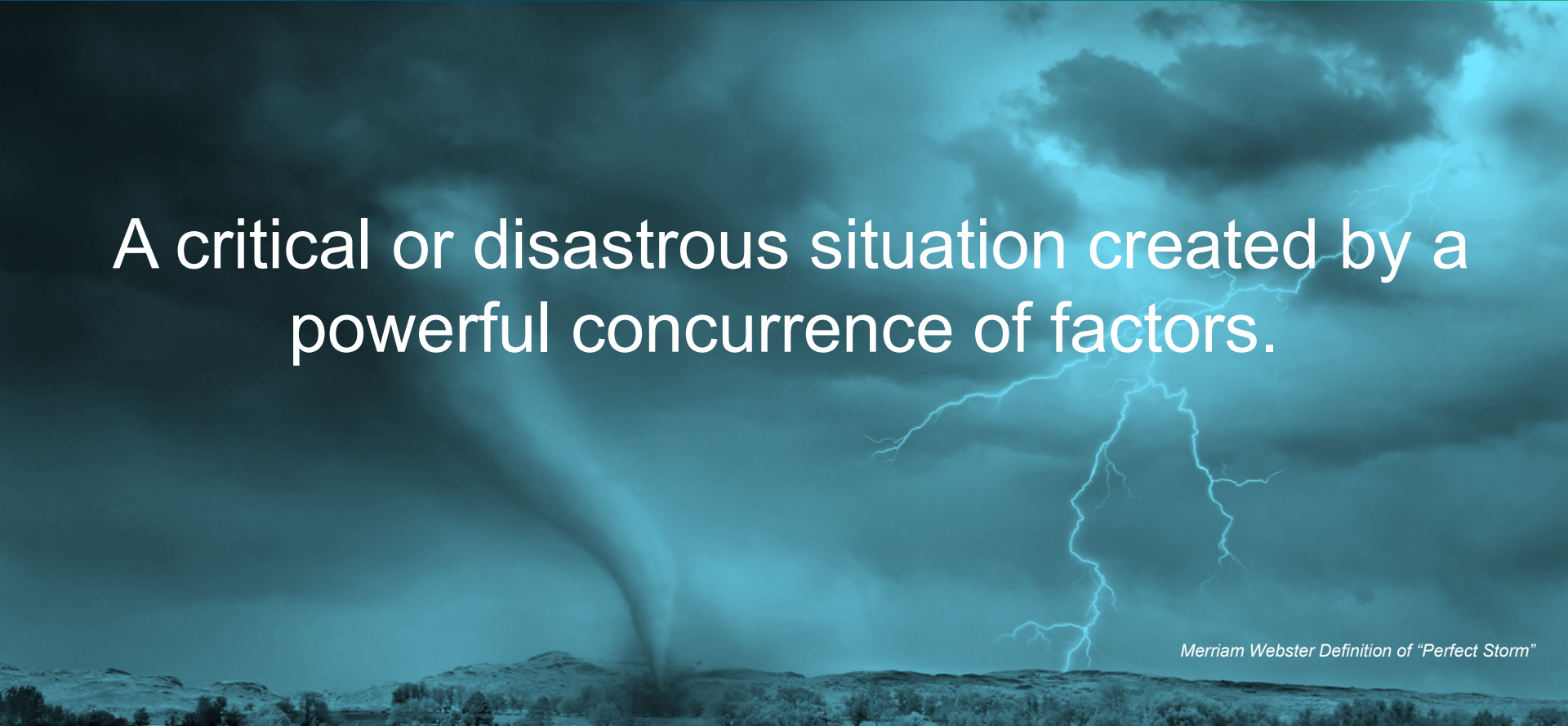
MOORE ClearComm

Why Schools?

Education and Cyber Crime: A Perfect Storm

A critical or disastrous situation created by a powerful concurrence of factors.

Merriam Webster Definition of "Perfect Storm"



Why Schools?



Large
Volumes
of Personal
Data

Inadequate
Security
Provisions

Lucrative
Rewards

Why Schools?

10,618,000 Students

Approximately 32,000 schools in the UK:

- 3,000+ nurseries or early-learning centres
- 20,000+ primary schools
- 4,000+ secondary schools
- 2,500+ independent schools
- 1,500+ special schools
- 50+ non-maintained special schools
- 340+ pupil referral units (PRUs)

Cantium Survey of 500 headteachers, school IT professionals and teaching staff:

- 37% “do not rank cyber security as a high priority”
- 66% worked in a school that had suffered a cyber-attack in the last 18-months
- Only 35% felt that they were:

“...well prepared to protect their school against malicious activity in the future.”

Question

UK schools are responsible for the data of
15.85% of the total population.

Many also (unnecessarily and unlawfully) store / process the data of former
pupils and staff, going back many years.

**What action is needed (by or on behalf of schools) to help them focus on
cyber risk and put adequate measures in place?**

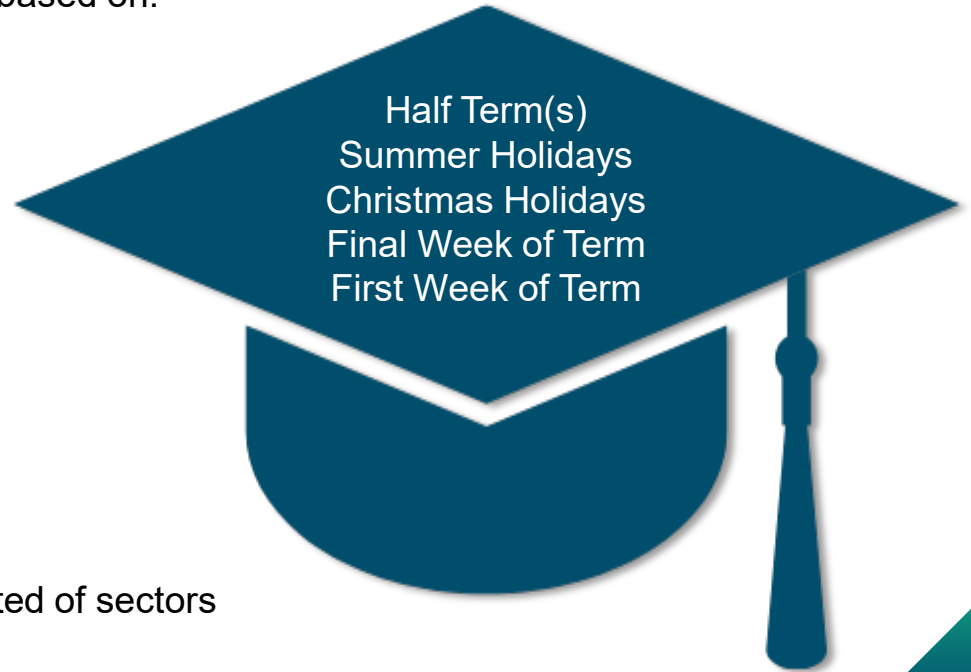
Seasonality

Seasonality Patterns

Cyber attackers specifically schedule attacks, based on:

- Increased pressure on staff
- Reduced diligence and “focus”
- Reduced resources and / or staffing
- Shutdowns / closures / skeleton staffing
- Especially busy or “distracting periods

Education is one of the most seasonality affected of sectors



Questions

What barriers or challenges might prevent schools from ensuring they have the best possible cyber defences in place?

Do school leadership teams fully comprehend the statistical likelihood of an attack on their school?



MOORE ClearComm

Awareness: The Essential First Step



MOORE ClearComm

Awareness: The Essential First Step

“The first step toward change is awareness.

The second step is acceptance.”

Nathaniel Branden



Awareness: The Essential First Step

- 1) Without awareness, we remain oblivious to the need for change
- 2) Without acceptance, we cannot implement lasting transformation

Step 3 = Action:


Acknowledgement that your school will be attacked in the next 1-3 years

- ✓ Understanding of the implications that a cyber event will bring with it
- ✓ Investment in adequate and appropriate technical defences
- ✓ Investment in the human elements of cyber awareness that will help staff to:
 - a) Maximise the chance of identifying a social engineering attack, and
 - b) Develop a collective culture of privacy and security, over time

Ground Zero Challenges

Key areas of focus for schools / education in 2024:

- Teaching staff recruitment and retention
- Safeguarding, mental health and wellbeing
- Student attainment
- Attendance
- Funding / budgetary challenges
- Technology / impact of AI
- Change of government



How can we ensure
that cyber security
and data protection
are prioritised?

Who needs to “own”
this in schools?



MOORE ClearComm

Case Studies

Case Study 1

- 14 UK schools impacted by a cyber-attack, resulting in confidential documents being leaked
- The data was originally stolen in 2022, with the data leaked online early in 2023 after schools failed to pay ransom demands
- Leaked data included:
 - ✗ Children's SEN information
 - ✗ Staff contract details / contract offer letters (including the headmaster's salaries)
 - ✗ Bursary fund receipts
 - ✗ Children's passport scans which had been used for school trips
- ✗ One folder marked "passports" contained passport scans for pupils and parents on school trips going back to 2011

Case Study 2

- London secondary school was attacked over May (2023) half term
- Closed for (at least) all the following week
- Only pupils taking GCSEs were currently able to attend the school
- Children in all other year groups were confined to home / remote learning
- ✗ IT systems were hacked / accessed and taken offline
- ✗ Significant” amount of personal data accessed
- ✗ The Single Central Record (SCR) was rendered inaccessible
- ✗ Not backed up, or with “cold” copies stored offline?

Department for Education - Guidance

- ✓ Ensure you have (at least) 3 backup copies of important data, on (at least) 2 separate devices
- ✓ At least 1 of these copies must be off-site, and 1 should be offline (referred to as a “cold backup”)
- ✓ Cold back-up should include the Single Central Record (SCR)
- ✓ Protect all devices on every network with a properly configured boundary or software firewall
- ✓ Network devices must be known / recorded, security features enabled, configured and up-to-date



Department for Education - Guidance

- ✓ Protect accounts with access to personal or sensitive operational data, using MFA
- ✓ Business Continuity and Disaster Recovery plans to be tested regularly, in response to cyber attacks
- ✓ All online devices and software must be licensed for use, and patched with the latest security updates
- ✓ Staff training: Ransomware and Phishing awareness, and key steps, actions and checks





EdSecure

EdSecure from MOORE ClearComm

- EdSecure is a new service launched specifically for schools
- Provides a blended Data Privacy and Cyber Security package of support
- Designed to reduce your risk, and to mitigate data breaches or cyber-attacks when they occur

Support can include:

- ✓ Cyber Essentials certification
- ✓ Data Privacy Helpdesk
- ✓ Data Privacy Advisory Service (DPAS)
- ✓ Department for Education Security Standards for Schools
- ✓ Digital Cyber Risk Report





MOORE ClearComm

Questions



richard.jackson@mooreclear.com



MOORE ClearComm

Our Next Webinar

Tipping the Scales: Cyber Guidance for Law Firms

Date: Thursday 26th September

Time: 10.00am-11.00am

Panel to be confirmed

Location: Zoom





MOORE ClearComm

Moore ClearComm

9 Appold Street

London

EC2A 2AP

t: +44 (0)20 45821983

www.mooreclear.com

Any assumptions, opinions and estimates expressed in the information contained in this content constitute the judgment of Moore Kingston Smith LLP and/or its associated businesses as of the date thereof and are subject to change without notice. This information does not constitute advice and professional advice should be taken before acting on any information herein. No liability for any direct, consequential, or other loss arising from reliance on the information is accepted by Moore Kingston Smith LLP, or any of its associated businesses.

Moore Kingston Smith LLP is regulated by the Institute of Chartered Accountants in England & Wales. Certain activities of the LLP and/or its associated businesses are authorised and regulated by the Financial Conduct Authority, the Financial Reporting Council or the Solicitors Regulation Authority. More details are available on our website at www.mooreks.co.uk © Moore Kingston Smith LLP 2024.



MOORE ClearComm