Student Loans Company

Cyber-Attacks: Minimising the Impact to Students, HEPs and SLC

Troy Ford

Kirsty Jordan

Contents

Student Loans Company

Data Sharing Agreement

A description of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

Contact details of the Data Protection Officer or other contact point where more information can be obtained;

A description of the likely consequences of the Personal Data Breach;

A description of the measures taken or proposed to be taken by the Processing Party to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects;

The Processing Party shall co-operate with the Controller Party and take such reasonable steps to assist the Controller Party in the investigation, mitigation and remediation of each such Personal Data Breach.

SLC
Student Loans Company

Question

- In the past 12 months, how many incidents has SLC responded to where HEPs have suffered a cyber-attack?

9

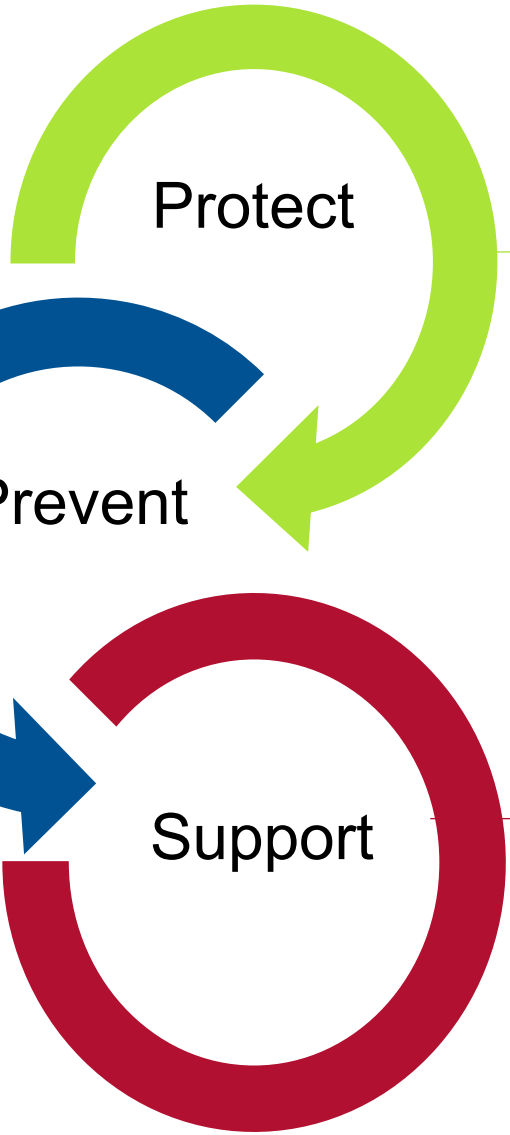
- What are the two most common types of cyber-attack that HEPs experience?

Ransomware

Exploitation of known vulnerabilities / poor security configuration

Student Loans Company

Why Do We Need To Know?



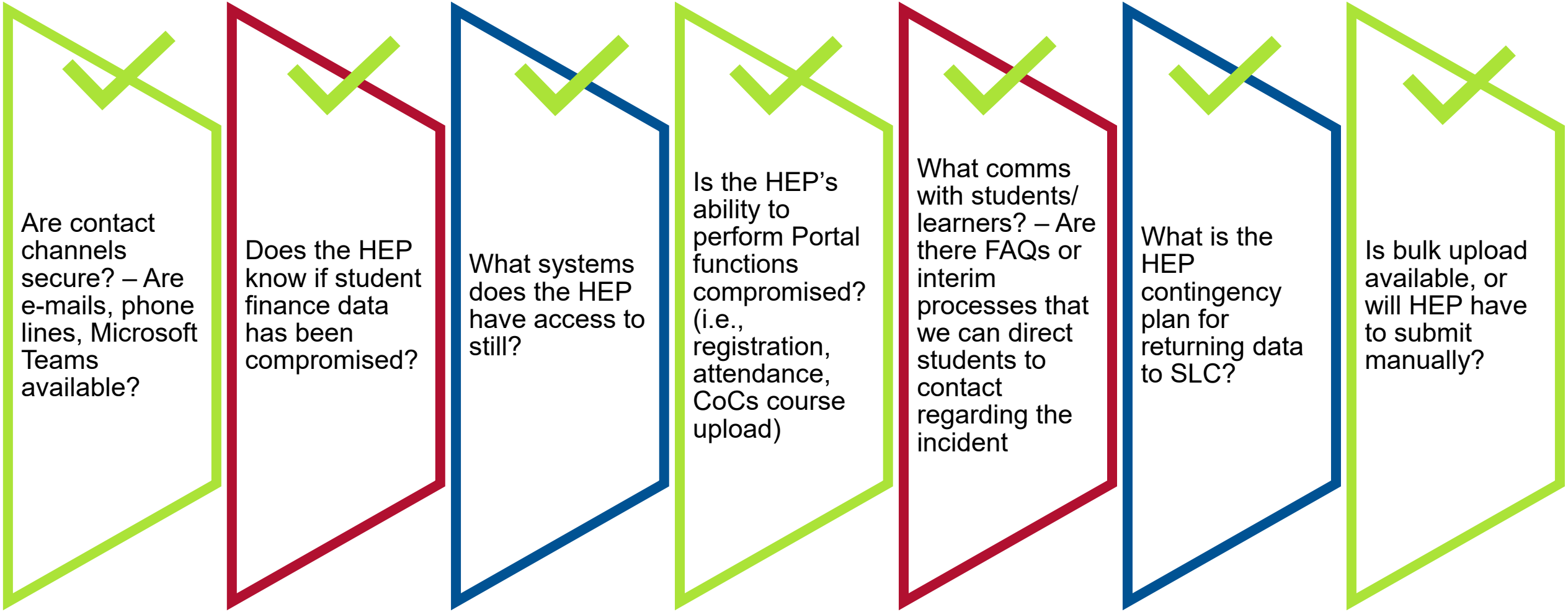
Protect SLC's IT Infrastructure

Prevent Data Loss

Provide Support to HEPs / Students

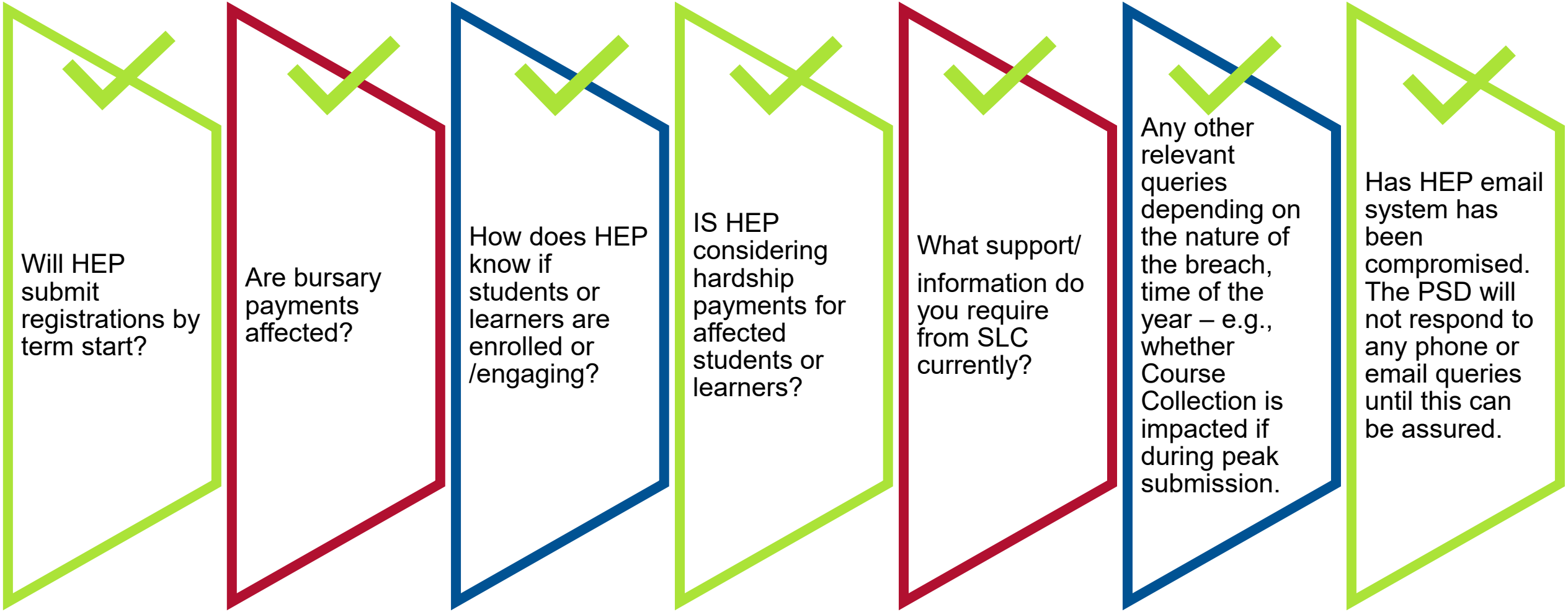
SLC
Student Loans Company

What Do We Need To Know?



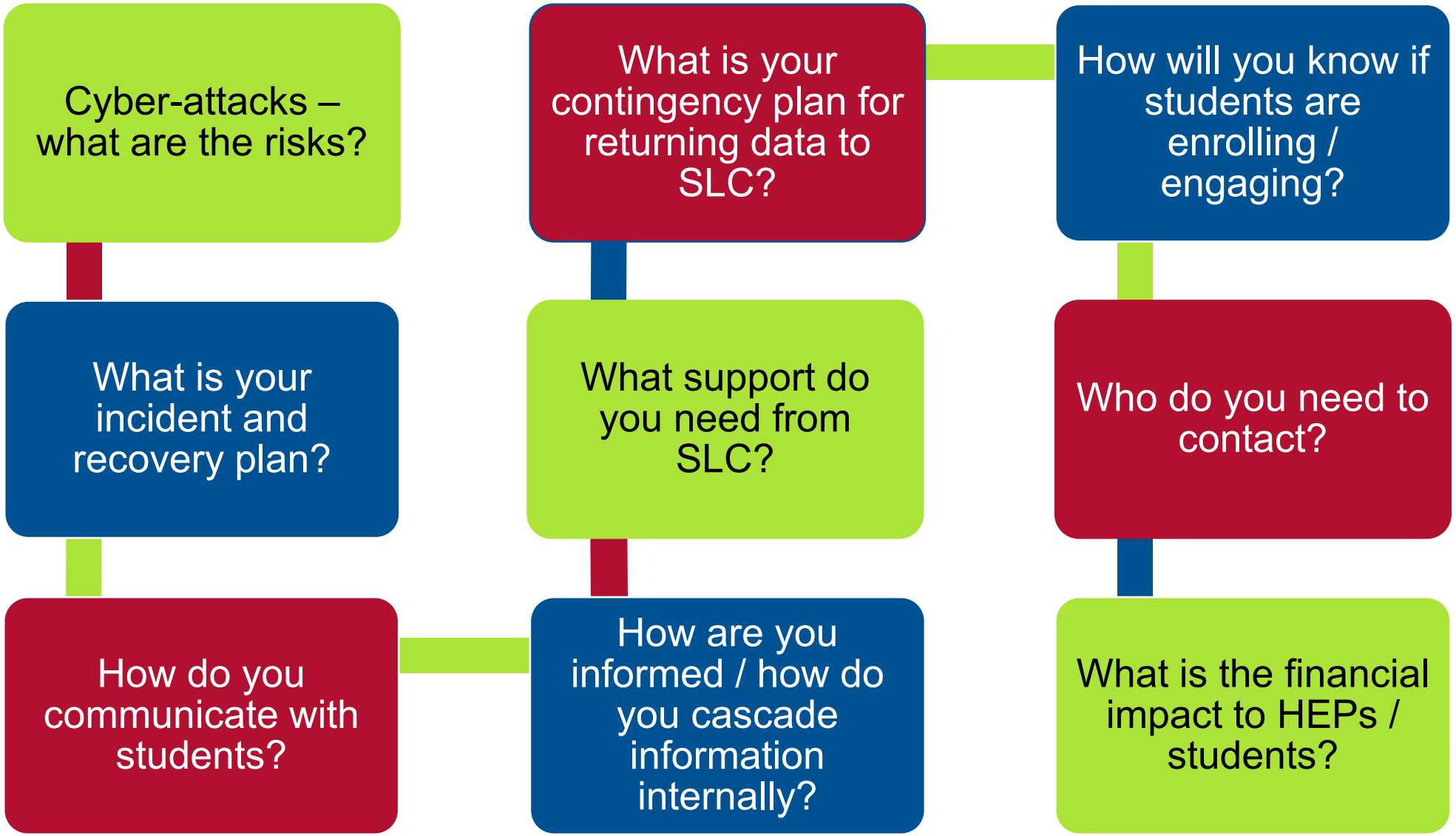
SLC
Student Loans Company

What Do We Need To Know?



SLC
Student Loans Company

Discussion



SLC
Student Loans Company

Case Study 1

A HEP had exposed a critical internal service to the internet through mis-configuration, allowing external attackers to exploit the service and gain a foothold to their network. The attackers then escalated their level of access to gain access to internal networks, leading to a widespread compromise and service outages.

How this would impact SLC

Educational Providers access SLC's HE and FE portals to confirm attendance of students and approve payment. The Provider's access via browsers and have restricted access which only allows them to modify information about their students and nothing more. They do have any privileged access and do not have perpetual direct access, therefore ransomware attacks in these institutions do not extend themselves to SLC systems.

A similar attack against SLC would not be successful as no critical services are exposed to the internet. SLC carries out regular penetration testing of externally facing systems and vulnerability scanning to ensure that any potential vulnerabilities/mis-configurations are identified and remediated.

In the event a service did become vulnerable and was exploited, SLC utilises a 24/7 managed SOC service that monitors for suspicious activity.

SLC
Student Loans Company

Case Study 2

A threat actor exploited a recently discovered vulnerability to gain access to a HEP network and uploaded ransomware which was then propagated throughout internal systems, leading to a widespread loss of service. A significant recovery effort is required to fully restore systems.

How this would impact SLC

SLC currently release new security updates for the majority of devices over a 10 day period, although this will take longer for some servers. In the event a vulnerability was rapidly exploited, SLC operates a number of protective and detective controls to stop ransomware from executing and gaining a foothold internally. This includes protection against more advanced techniques that are currently being used by some ransomware variants.

If ransomware did execute, SLC has a defined and practised response and recovery process to mitigate the existing threat and recover from backups if required. This is an area that is currently being developed to further mature the overall capability, including running regular Incident Response exercises and a programme of work focussing on Disaster Recovery.

SLC
Student Loans Company

Question time