Information Security & Data Protection in the Games Industry

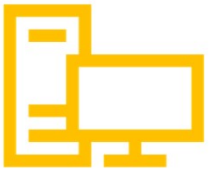
Andrew Montgomery


Privilege
Classification
Compensating
Interruption
Impact
Risk
Qualitative
Recovery
Incident
Strategic
Encryption
Personnel
Theft
Handling
Exploitation
Administrator
Engineering
Regulation
Vital
Walkthrough
Dissemination
Penetration
Sensitive
Asset
Appetite
Laptop
Policy
Failures
Continuity
Replay
Metric
Detective
Cracking
Mitigation
Zone
Hash
Deterrent
Neural
Retain
Failed
Authentication
Disaster
Property
Intellectual
Likelihood
Tolerable
Biometric
Backups
Destruction
Accidents
Social
Executive
Procedure
Tolerance
Hacking
Restoration
Service
Inventory
Liability
IP
Integrity
Nonrepudiation
Viruses
Audit
Defense
Authorization
Event
Trust
Reciprocal
Evaluation
Simulation
Availability
Management
Lost
Diligence
Fires
Due
Baseline
System
Control
DoS
Insurance
Critical
Intentional
Quantitative
Transference
Access
Spoofing
Denial
Residual
Repudiation
Vulnerability
Confidentiality
Permission
Attacks
Custodian
Fraud
Compliance
Eavesdropping
Scanning

Fundamentals of Computer Security

What is computer security?

Why is computer security so important?



Why is computer security so difficult?

What Does Security Mean?

The term security is used in a variety of contexts. What's the common thread?

- Personal security
- Physical security
- Operational security
- Communications security
- Network security
- System security
- National security

What Does Security Mean?

security

sɪˈkjʊərɪti,sɪˈkjɔːrɪti

noun

1. the state of being free from danger or threat.

   "the system is designed to provide maximum security against toxic spills"

   synonyms: certainty, safe future, assured future, safety, reliability, dependability, solidness, soundness

- What assets do we have?
- What kinds of threats do we face?
- What does “protection” mean?
- Is the type of protection needed dependent on the type of threat?

Security on a Personal Level

If you visit an online shop and need to enter personal details ...

What protections do you expect?

And from what threats?

- Authentication (protection from phishing)
- Authorisation
- Privacy of your data
- Integrity of your data
- Availability
- Non-repudiation- what is this?
- What else?

Security on an Institutional Level

Think about the situations below:

- **A big company's computer systems are hacked with personal and financial data on thousands of customers being stolen.**
- **A student hacking into the University of Brighton's registrar system and changing his/her grades in modules he/she had taken.**
- **An online shopping site is overwhelmed by a denial of service attack, making it unavailable for authentic customers to buy goods**

Is it hard to define 'security' in the context of digital systems?

Computer Misuse Act 1990, s2

R v Imran Uddin	Birmingham Crown Court 24 April 2015	Adult student at University of Birmingham installed four keyboard spying devices to steal staff passwords used to obtain access to his examination results and improve grades. Guilty plea to six CMA charges - unauthorised access to computer material, intent to commit further offences and impairing the operation of a computer. Four-month prison sentence.


Uddin attached a device called a 'keylogger' to computers used by staff at the University of Birmingham
The keylogger is attached to the cable that connects the PC to the keyboard
The device records all of the keyboards activities and logs them
Once the log was retrieved Uddin could use the recorded passwords to log in to the university's computer system and manually alter his exam results

Computer Misuse Act 1990, s2

R v Imran Uddin https://www.dailymail.co.uk/news/article-3053639/Cheating-student-hacked-university-computer-better-degree-jailed.html

Recent Attacks

- Fortnum & Mason shoppers' details stolen in data breach
- Ticketmaster admits customer data may have been stolen in malware attack
- Data of hundreds of RNIB customers might have been stolen by hackers
- Thousands of Lloyds customers have personal data stolen
- Barclays blasted over 'catastrophic' theft of thousands of customer files
- Pizza Hut hack: Thousands of customers' data stolen as users report fraudulent card transactions
- Hackers strike at Vodafone stealing bank details from thousands of customers
- Tesco Bank: How was £2.5m stolen from customers' accounts?
- TalkTalk given record fine over data breach that led to data theft of nearly 157,000 customers

Sony's PlayStation Network
Date: April 20, 2011

- Impact: 77 million PlayStation Network accounts hacked
- Estimated losses of $171 million while the site was down for a month
- Details: This is viewed as the worst gaming community data breach of all-time
- Of more than 77 million accounts affected, 12 million had unencrypted credit card numbers
- Hackers gained access to full names, passwords, e-mails, home addresses, purchase history, credit card numbers and PSN/Qriocity logins and passwords.
  - "It's enough to make every good security person wonder, 'If this is what it's like at Sony, what's it like at every other multi-national company that's sitting on millions of user data records?'" said eIQnetworks' John Linkous. He says it should remind those in IT security to identify and apply security controls consistently across their organizations. For customers, "Be careful whom you give your data to. It may not be worth the price to get access to online games or other virtual assets."
- In 2014, Sony agreed to a preliminary $15 million settlement in a class action lawsuit over the breach

Lulzsec and Anonymous have been hacking games companies

high-profile attacks on, among others …

Nintendo

Sony

Bethesda

Codemasters

Minecraft

Why are Attacks Becoming More Prevalent?

INCREASED CONNECTIVITY

RELATIVELY EASY TO ACCESS

MANY MORE HOSTS ONLINE (IOT)

MANY MORE SOPHISTICATED HACKING TOOLS AND METHODOLOGIES EXIST

OTHER REASONS?

Some Sobering Facts

- Between October 2016 and the end of 2017, the NCSC recorded 34 significant cyber attacks
  - attacks that typically require a cross-government response), with WannaCry the most disruptive of these.
- 762 less serious incidents (typically confined to single organisations) were also recorded. 2018 will bring more of these attacks.
- The Internet of Things and its associated threats will continue to grow and the race between hackers' and defenders' capabilities will increase in pace and intensity.

- The Cyber Threat to UK Business (National Cyber Security Centre)

Educate Yourself

Learning about computer security can:

- improve your own protection
- help with security in the workplace
- improve the quality and safety of your personal and business transactions
- improve overall web security

10 Steps To Cyber Security: At-a-glance (NCSC)

An effective approach to cyber security starts with establishing an effective organisational risk management regime

- shown at the centre of the following diagram

This regime and the 9 steps that surround it are described below

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to **www.ncsc.gov.uk** **@ncsc**

Risk Management Regime

Embed an appropriate risk management regime across the organisation.

This should be supported by an empowered governance structure, which is actively supported by the board and senior managers.

Clearly communicate your approach to risk management with the development of applicable policies and practices.

These should aim to ensure that all employees, contractors and suppliers are aware of the approach, how decisions are made, and any applicable risk boundaries.

Secure Configuration

Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems.

You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching.

Failure to do so is likely to result in increased risk of compromise of systems and information.

Network Security

The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack.

By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation).

Your organisation's networks almost certainly span many sites and the use of mobile or remote working, and cloud services, makes defining a fixed network boundary difficult.

Rather than focusing purely on physical connections, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

Managing User Privileges

If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be.

All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role.

The granting of highly elevated system privileges should be carefully controlled and managed.

This principle is sometimes referred to as ‘least privilege’.

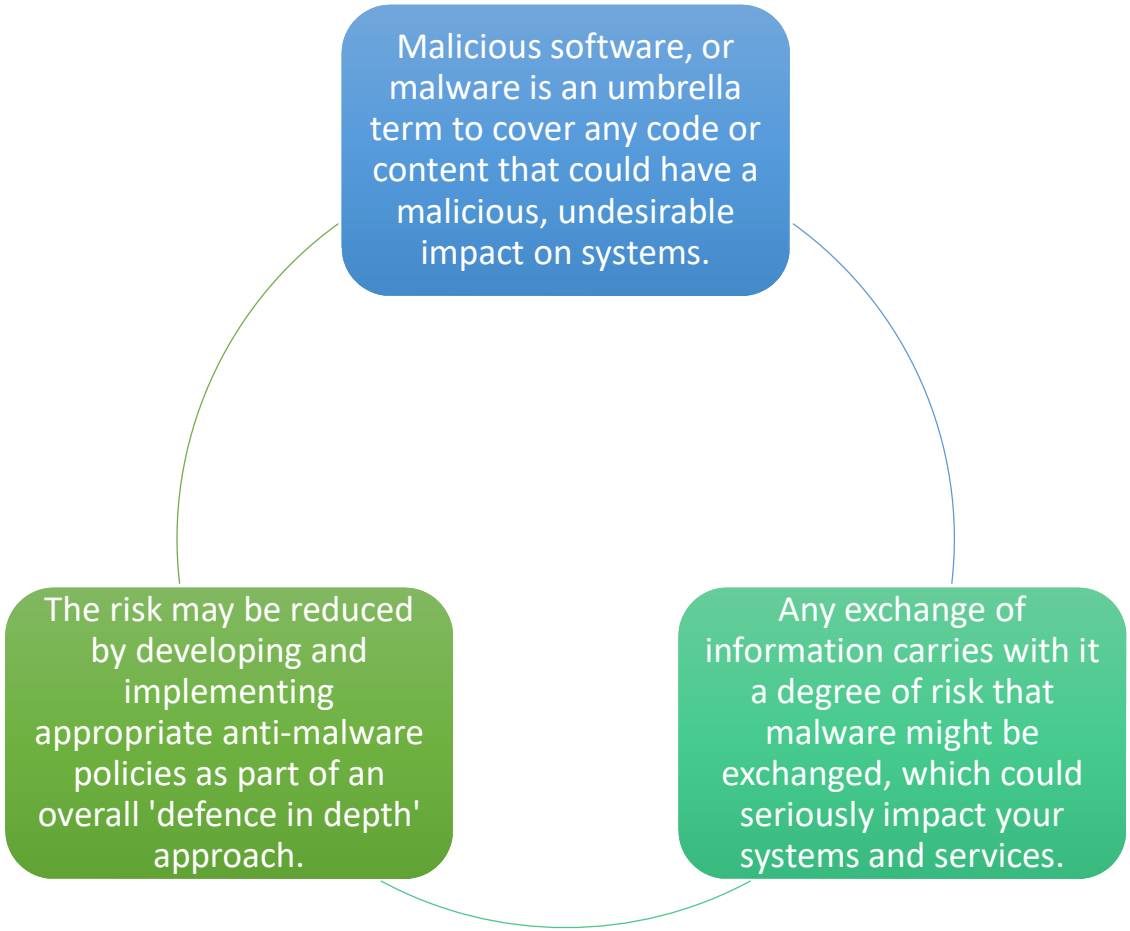
User Education and Awareness

Users have a critical role to play in their organisation’s security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure.

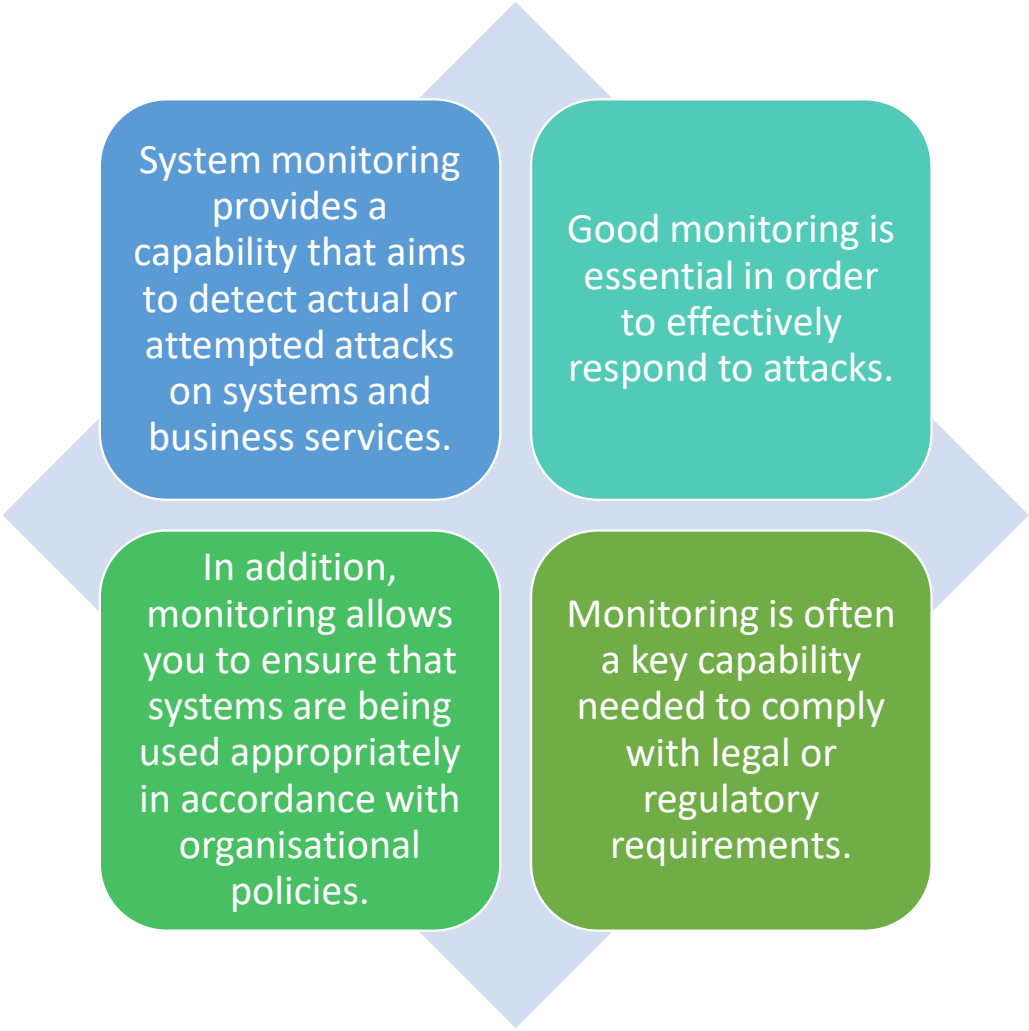
This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture.

Incident Management

Malware Prevention



Monitoring


System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services.
Good monitoring is essential in order to effectively respond to attacks.
In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies.
Monitoring is often a key capability needed to comply with legal or regulatory requirements.

Removable Media Controls

Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data.

You should be clear about the business need to use removable media and apply appropriate security controls to its use.

Home and Mobile Working

Mobile working and remote system access offers great benefits but exposes new risks that need to be managed.

You should establish risk-based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers.

Train users on the secure use of their mobile devices in the environments they are likely to be working in.

The GDPR

Following the introduction of the General Data Protection Regulation in 2016, a two-year transition period was granted before enforcement began on 25th May 2018.

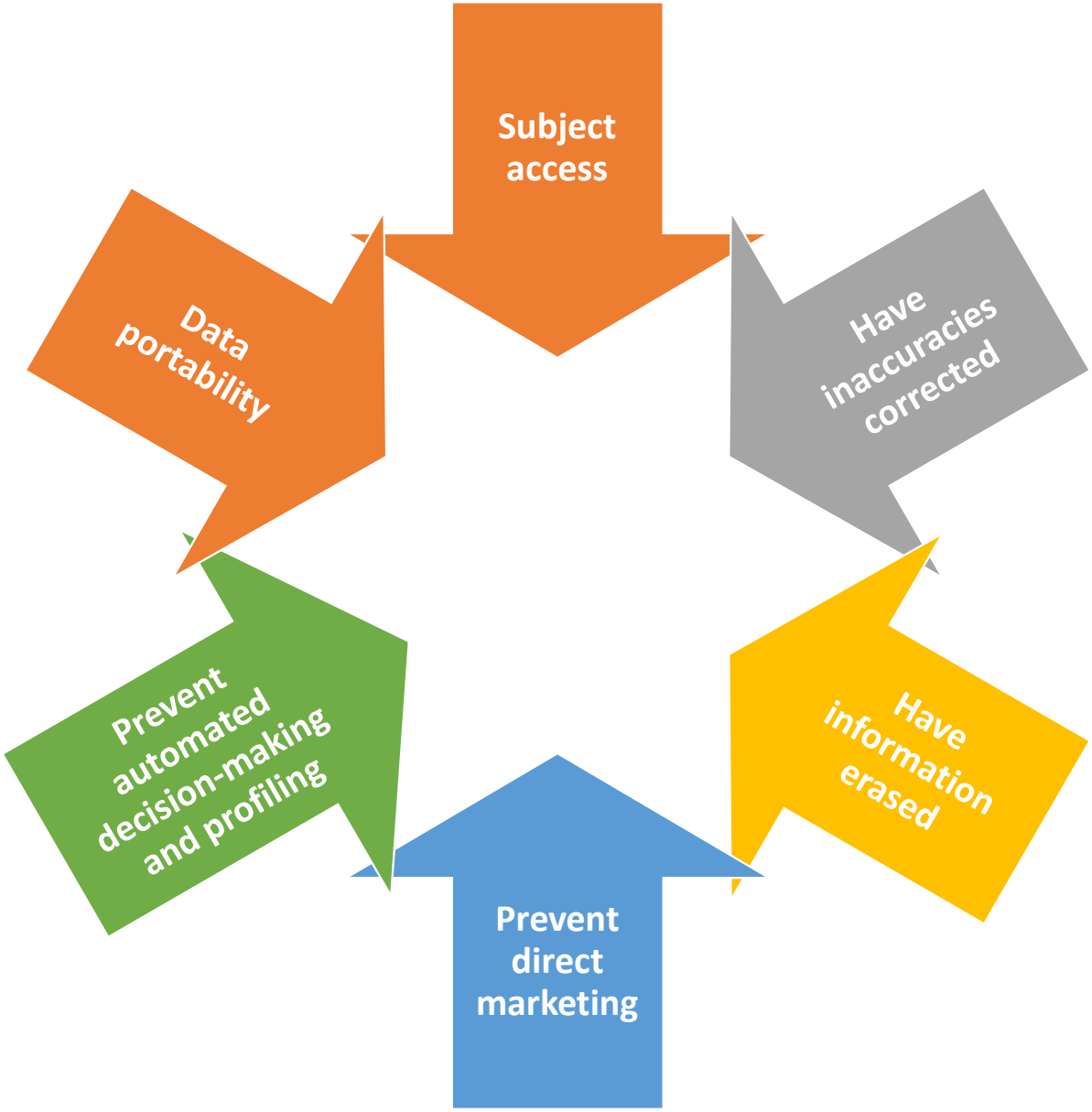
During that time, organisations involved in the processing of personal data reviewed their strategy, policies and procedures for compliance.

At the same time, consumers have become aware of a new set of rights which they have been granted by GDPR

Things have changed!

When getting consent to process individuals' personal data, you must be able to demonstrate that this consent was "freely given, specific, informed and unambiguous".

Under the GDPR, individuals' rights have been enhanced. These include rights to:



Personal data is data relating to living individuals, whether hard or soft copy, for example in research this could be:

Names, contact details, other factual information

Answers to questions, for example in questionnaires or interviews, whether factual or opinion

Names and signatures on consent forms

Photographs, film, video, audio, transcripts of interviews etc.

Test results of a personal nature

Personal Data –
How will you deal with that data?

PROVIDING ENOUGH INFORMATION AND GAINING CONSENT

SECURITY OF THE DATA

RETENTION OF THE DATA

DISPOSAL OF THE DATA

CONFIDENTIALITY OF THE DATA

ANONYMISING DATA

PROPER USE OF DATA

Provide enough information and gaining consent

Gain consent for collecting and processing the data

Create a participant consent form

Provide enough information about the project for the participant to be able to give informed consent

Participant information sheet should include:

Enough information, in lay language, for the participant to understand what the project is about and what is required of them so that they can give informed consent

Who they can contact for more information (business contact details) and who is the organisation overseeing the research

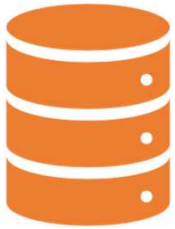
A date by which participants are able to withdraw their data from the study

Assurances that their data will be held securely and treated correctly.

Security of the data

Hold	Be	Do not share	Be	Transfer	Guard
Hold it in a secure location, whether electronic or hard copy • Locked cabinet, password-protected files and shared drives, encrypted lap-top	Be particularly aware of movable storage media, e.g. USB sticks, lap-tops	Do not share the data except with co-researchers	Be aware if you are carrying or transferring data abroad, particularly outside the EEA	Transfer the data in a secure manner • Package and address correctly, avoid email if possible	Guard against unauthorised access or accidental loss, damage, or destruction of the data

Retention and Disposal of Data



Retention of the data

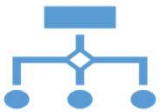
Decide how long you need to keep it, and for what reason. Don't keep it any longer than necessary

Decide how long you need to keep the administrative records associated with the project, and for what reason. Don't keep them any longer than necessary

Disposal of the data

Dispose of it securely, whether electronically or in hard copy

Confidentiality of the Data



Anonymise the data once collected, for example:

- Separate the data from the identifying details of the participant

- Give the data a code and attach the code to the separate contact details

- Allow participants to choose codes / passwords so that they could be allowed access to their data if necessary / withdraw from the project within certain timescales

Ensure that data is published only in anonymised form

- Ensure that the data never causes damage or distress to individuals

- Ensure that it is never used to support measures or decisions relating to particular individuals

Never use the data you have collected, nor the contact details of participants, for another purpose other than a research purpose

Any Questions?

Sources

- https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security
- The UoB Project Handbook
- http://www2.gre.ac.uk/research/ethics/what-might-be-the-ethical-issues-and-risks-that-arise-in-my-research
- https://www.nottingham.ac.uk/educationstudentintranet/researchethics/data-protection-act.aspx
- https://www.jisc.ac.uk/blog/a-year-to-get-your-act-together-how-universities-and-colleges-should-be-preparing-for-new-data-regulations