CampusGuard News 9/1/2018

Data Privacy vs. Data Security

The terms “data privacy” and “data security” are often confused or used interchangeably. It is important to not only understand the difference between the two, but to understand how they correlate as you are developing your information security, privacy, and compliance programs.

Privacy, at a high level, is the right of individuals to keep their personal information from being disclosed or accessed by those who have no need to have that information. Your customers – students, faculty, staff, alumni, donors, patients, vendors, etc. – all trust and assume that their personal information will be kept confidential (and your privacy notices should be communicating to them that this will happen as well).

A robust data privacy program will explicitly control who is authorized, by individual and by role, to access sensitive information. Definitions will also include the conditions under which that information may be accessed, how it can be used, and if/how it will be shared with any third-parties.

When you think of privacy in your environment, you should ask:

- What sensitive data is being collected?
- What are the permissible uses of that data?
- Who should have access to the data and with whom can it be shared?
- How long should the data be retained?

Privacy controls are typically implemented through policy and procedure, and often based on individual privacy rights regarding different types of restricted or sensitive data as dictated by law or regulation (i.e. FERPA, HIPAA, GLBA, GDPR, etc.). Responsibility for data privacy usually falls with an organization’s compliance office. The compliance officer and/or team ensures that people are aware of the legal requirements and privacy risks related to the handling and dissemination of personal data.

Data security on the other hand, is how the data is protected at all stages – when it is being collected, when it is stored, and how it is destroyed. Data security includes all of the safeguards and controls that must be implemented to allow or restrict access to the information, as well as to protect from the unauthorized disclosure, theft, alteration, loss, or destruction of this data. Security encompasses the technical safeguards your organization should have in place such as firewalls, virus protection, and password/access controls, and physical safeguards like locks, cameras, information destruction/shredding, etc.

Data privacy defines “who”, “what”, and “when” individuals can access data, but security defines the “how” or the protocols that allow these authorized individuals to access information when they need it,

and blocks unauthorized access from occurring. Privacy-related requirements, once documented, should be passed along to the security team to implement appropriate technologies and controls. In effect, you can't implement a successful privacy program without the support of a comprehensive security program. If someone can steal your personal data due to a lack of security, then your privacy can not be guaranteed. A recent example of this was reported by KrebsOnSecurity on August 28th when technology services company Fiserv, Inc., accidentally exposed the personal and financial data of bank customers by failing to properly secure their web platform.

https://krebsonsecurity.com/2018/08/fiserv-flaw-exposed-customer-data-at-hundreds-of-banks/

Yes, in theory, you could potentially implement security controls and still fail to protect data privacy. For example, your security program could require secure access credentials to log into the network but then fail to restrict access to the data on the network. You would have security, but no privacy, as any user with valid credentials could see all of the sensitive information your organization possesses.

With technology changing rapidly, and new risks constantly emerging, there is a constant struggle to balance security and privacy. Keeping the unique goals of each in mind when defining your overall program will maximize the strength of your program and better protect your customer data.

Some additional guidance from the Security Advisor Team below:

> **[Burt]:** *No matter what kind of data is involved (e.g. payment card numbers, social security numbers, personal health information, etc.), when it belongs to someone that person has the right to assume their information is being treated as sensitive/confidential.*
>
> *The PCI DSS, NIST SP 800-53, NIST SP 800-171 and SANS CIS 20 are examples of standards that assist in assuring data and systems are implemented and maintained in a secure manner. At a high level, privacy is the right for information to be protected and security is the method of such protection. Whether its payment card data or other regulated data, an organization can assure it's taking appropriate measures to satisfy and comply by implementing a solid Information Security program.*