Global Scientific JOURNALS

GSJ: Volume 7, Issue 1, January 2019, Online: ISSN 2320-9186

www.globalscientificjournal.com

DATA SECURITY ENHANCEMENT OF AN ORGANIZATION TO OPTIMIZE THE OPTIMAL PROTECTION OF THE DATA INTEGRATION

Syed Jamaluddin Ahmad, Roksana Khandoker, Tasnim Niger, Farzana Nawrin

Abstract:
The world is moving to a different dimension. Technology is conquering all aspects of our daily lives. When we say technology it essentially means "Data". Unprotected data management paves the opportunity of data security breach resulting to massive financial and reputational loss.
Large organization and different governments are spending millions of dollars to ensure data security. Currently we are seeing many organization are facing a lot of challenges from the regulators for breach of data security which is resulting of leakage of human personal data. For large organization it the utmost responsibility to ensure an optimal protection of data integration. There are multiple ways of ensuring data security which keeps on evolving as the technology is advancing. Here we entails highlighting various types of data security breach and enhancement of data security across the organization.

Syed Jamaluddin Ahmad, Assistant Professor and Head, Department of Computer Science & Engineering, Shanto-Mariam University of Creative Technology, City: Dhaka, Country: Bangladesh,
Mobile No.: +8801708090739 (Email: jamal35@gmail.com)

Roksana Khandoker, Senior Lecturer, Department of Computer Science & Engineering, University of South Asia, City: Dhaka, Country: Bangladesh, Mobile No.: +8801737157856

Tasnim Niger, Lecturer, Department of Computer Science & Engineering, Shanto-Mariam University of Creative Technology, City: Dhaka, Country: Bangladesh, Mobile No.: +8801731222452

Farzana Nawrin, Lecturer, Department of Computer Science & Engineering, Shanto-Mariam University of Creative Technology, City: Dhaka, Country: Bangladesh, Mobile No.: +8801686521152

Definition of Data Security:

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is an essential aspect of IT for organizations of every size and type.
Data security is also known as information security (IS) or computer security.
Examples of data security technologies include backups, data masking and data erasure. A key data security technology measure is encryption, where digital data, software/hardware, and hard drives are encrypted and therefore rendered unreadable to unauthorized users and hackers.
One of the most commonly encountered methods of practicing data security is the use of authentication. With authentication, users must provide a password, code, biometric data, or some other form of data to verify identity before access to a system or data is granted.

Data security is also very important for health care records, so health advocates and medical practitioners in the U.S. and other countries are working toward implementing electronic medical record (EMR) privacy by creating awareness about patient rights related to the release of data to laboratories, physicians, hospitals and other medical facilities.

Data masking:

Data masking refers to the process of changing certain data elements within a data store so that the structure remains similar while the information itself is changed to protect sensitive information. Data masking ensures that sensitive customer information is unavailable beyond the permitted production environment. This is especially common when it comes to situations like user training and software testing.

Automated development and testing methods cut down direct exposure to sensitive data. Even so, there are many situations where data is required. Take for, example, a bank that has outsourced some development to foreign companies. It is often illegal for customer information to leave the bank, never mind the country in which the bank is regulated. By using a technique like data masking, the off shored development firm can test the software with data that is similar to what would be experienced in the live production environment.

Potent data masking necessitates the modification of data so that the original values are not re-engineered or identified. Data could be encrypted and decrypted, relational integrity is sustained, safety polices can be proved, and separation of duties between administration and security can be started.

Health Care Data Encryption

Before the Health Information Technology for Economic Clinical Health (HITECH) Act was enacted in 2009, only two states in the U.S. implemented data breach requirements in patient health data. California was one of the two states, but 800 reports of personal health information (PHI) data breaches still occurred there in the first five months after HITECH was enacted. This points to the importance of PHI data security, especially in light of the fact that health care providers can now be fined for breaches of their electronic data. When the Health Insurance Portability and Accountability Act (HIPAA) was implemented in 2003, it did not mandate PHI data encryption. But much has changed since then.

Consideration of EHR data encryption is wise for health care providers, administrators, IT personnel and health facilities. Although encryption is not foolproof, it's better than plain text records. And although much attention has been paid to national laws such as HITECH as far as paper medical records conversion and guidelines for EHRs, less attention has been given to Department of Health and Human Services (HHS) regulations in which data destruction or data encryption are the only two forms of protection for patient health data. In addition, should one or the other of these forms of protection be enlisted, the mandate to notify patients of data breaches is waived. However, critics feel that any breach should be reported, whether data has been encrypted or not.

Electronic Health Record (EHR)

An electronic health record (EHR) is an automated, paperless and online medical record for which patient medical data is entered by eligible providers (EP), such as nurses and physicians. An EHR contains valuable and pertinent automated medical information, including:

- Patient vitals
- Prescriptions
- Medical histories

- Diagnoses
- Surgical notes
- Discharge summaries

While EHRs are meant to be shared by EPs for enhanced patient treatment and less human medical error, as well as cost containment, many EHR concerns and complexities arise when considering privacy issues, especially regarding sensitive health data, such as behavioral health information.

Electronic health records are also known as electronic medical records (EMR).

Electronic health records may be viewed by other patient care EPs, as well as patients. Although EHRs are designed to further interoperability or health information exchanges (HIE), IT personnel must work to tailor databases to prevent the automatic release of sensitive data for the preservation of doctor-patient relationships, as well as secure data to prevent release to marketing firms and malicious types of unauthorized users. Privacy advocates believe EHR vendors do not provide proper database security. To combat this serious issue, privacy protection laws are continuously gaining legislative support, as existing regulations do not entirely take into account protected health information (PHI).

EHR implementation is required by law under the American Recovery and Reinvestment Act (ARRA) of 2009, also known as the Stimulus Act, by the year 2015, for all U.S. health care organizations claiming Medicare/Medicaid reimbursement and incentive payments. Many expect this deadline to be extended due to the difficulty of nationwide implementation. Those that find EHR implementation most arduous are small private practices without ample IT resources and rural-based health facilities. EHR implementation began long before legislative requirements were established for teaching hospitals, large enterprises and other health care organizations that typically have a plethora of IT professionals.

Hacker

Hacker is a term that refers to many different computing topics. However, in the mainstream, a hacker is any individual or group that circumvents security to access unauthorized data.

Most hackers are highly skilled computer programmers that locate security gaps and access secure systems via unique analytical skills. A great hacker is known to be able to "think outside the box."

Hacker types are delineated according to intent, as follows:

Black hat hackers break into computer systems illegally and cause harm by stealing or destroying data, i.e., a banking system to steal money for personal gain.
White hat hackers use their skills to help enterprises create robust computer systems.
Grey hat hackers perform illegal hacking activities to show off their skills, rather than to achieve personal gain.

Exploit

The term is very flexible and can be used both as a noun as a verb. As a noun, the exploit is the hole in the system that the hacker used to make the attack. Quite often, this is an OS vulnerability from an unpatched server. As a verb, it refers to the act. For example, you might hear "the hacker posted details of his exploits on his blog to show just how easy it was to break into XYZ's servers."

Information Assurance (IA) mean?

Information Assurance (IA) refers to the steps involved in protecting information systems, like computer systems and networks. There are commonly five terms associated with the definition of information assurance:

- Integrity
- Availability
- Authentication
- Confidentiality
- Nonrepudiation

IA is a field in and of itself. It can be thought of as a specialty of Information Technology (IT), because an IA specialist must have a thorough understanding of IT and how information systems work and are interconnected. With all of the threats that are now common in the IT world, such as viruses, worms, phishing attacks, social engineering, identity theft and more, a focus on protection against these threats is required. IA is that focus.

Essentially, Information Assurance is protecting information systems through maintaining these five qualities of the system.

Integrity involves making sure that an information system remains unscathed and that no one has tampered with it. IA takes steps to maintain integrity, such as having anti-virus software in place so that data will not be altered or destroyed, and having policies in place so that users know how to properly utilize their systems to minimize malicious code from entering them.

Availability is the facet of IA where information must be available for use by those that are allowed to access it. Protecting the availability can involve protecting against malicious code, hackers and any other threat that could block access to the information system.

Authentication involves ensuring that users are who they say they are. Methods used for authentication are user names, passwords, biometrics, tokens and other devices. Authentication is also used in other ways -- not just for identifying users, but also for identifying devices and data messages.

IA involves keeping information confidential. This means that only those authorized to view information are allowed access to it. Information needs to be kept confidential. This is commonly found, for example, in the military, where information is classified or only people with certain clearance levels are allowed access to highly confidential information.

The final pillar is no repudiation. This means that someone cannot deny having completed an action because there will be proof that they did it.

Hacking Tool

A hacking tool is a tool or program that is specially designed to help a hacker. The true meaning of hacking is derived from “hacking away”, which is used to refer to someone who is extremely proficient in computer technology and hacks away at the bits and bytes. Today’s definition of hacking refers to a self-taught prodigy or specialized programmer who is able to modify computer hardware or software outside a developer’s architectural design.

Black Hat Hacker

The term "black hat hacker" is derived from old Western movies, in which the good guys wore white hats and the bad guys wore black hats.

Black hat hackers can range from teenage amateurs who spread computer viruses to networks of criminals who steal credit card numbers and other financial information. Black hat hacker activities include planting keystroke-monitoring programs to steal data and launching attacks to disable access to websites. Malicious hackers sometimes employ non-computer methods to obtain data, for example, calling and assuming an identity in order to get a user's password.

Black hat hackers have their own conventions, of which two of the more

prominent are DEFCON and BlackHat. Black hat conventions are often attended by security professionals and academics who want to learn from black hat hackers. Law enforcement officials also attend these conventions, sometimes even making use of them to apprehend a black hat hacker, as occurred in 2001 when a Russian programmer was arrested the day after DEFCON for writing software that decrypted an Adobe e-book format.

Ethical Hacker

Generally, a software or hardware vendor achieves greater profitability by hiring ethical hackers, versus being subjected to other types of vulnerabilities and exploitations.

Ethical hackers evaluate systems using a number of methods, some of which include:

- Denial of Service (DoS) attacks: These are usually applied by flooding a system with requests, rendering it unable to handle additional requests, which halts service to other users or results in system overflow and/or shutdown.
- Social Engineering tactics: Akin to simple fraud, these include any act that manipulates a user into divulging information or performing specific actions.
- Security scanners: Used to discover vulnerabilities, security scanners are exploitation tools designed to discover vulnerabilities in networks.

Mode of Attack

The following are historical examples of damaging viruses and their modes of attack:

- Morris 1988: Exploited email client flaws in Unix Sendmail.
- Melissa 1999: Forced the shutdown of email gateways by generating excess traffic.
- VBS/Loveletter 2000: Exploited email address lists and sent large numbers of messages.
- Code Red 2001: Exploited a buffer overflow and damaged connectivity.
- Nimda 2001: Generated masses of email to transmit itself, lured users to an infected website and exploited issues with security software.
- SQL Slammer 2003: Exploited buffer-overflow bug and distributed copies of itself worldwide, causing service denials and Internet slowdown.
- MS Blaster 2003: Exploited MS windowsupdate.com, causing major denial-of-service attacks and forcing computer restarts for banks, city governments and thousands of home and corporate users.
- MyDoom 2004: A virus spread via email attachment. The virus spread when the attachment was opened and exploited address book lists. It also exploited the Kazaa file-sharing service.
- Sasser 2004: Exploited buffer-overflow and affected transportation. Delta canceled 40 trans-Atlantic flights and Australian trains were forced to halt operations.
- Witty 2004: Exploited network vulnerabilities by attacking network-protection software. It overwrote hard disks, rendering them unusable.

Trusted Data Format (TDF)

The Trusted Data Format is, more or less, a protective wrapper that contains the user's data. It is an open standard designed to control all types of data security. The TDF allows selective access control for files and add-ons, including email attachments, PDFs, office files, videos and other multimedia files. The basic purpose of this format is to offer a resilient but flexible security and encryption format that is user-friendly for a wide variety of users. A number of privacy

control applications were developed on this standard including those created for easy-to-use end-to-end email encryption service.

5 Ways to Enhance Data Security

The world of cybersecurity is progressing at a huge speed and in at the same time, improvements in technologies are becoming increasingly better at assisting the hackers and cyber-criminals to exploit data security loopholes. The constant increasing graph of cybersecurity attacks are a major concern for internet users and business organizations. And they should be!

One recent example of the growing scale of such attacks is the recent ransomware attack known as WannaCry. It was one of the largest attacks in recent years affecting a large number of businesses all over the world. Here's where the question arises; 'why have both large and small businesses been affected and influenced by this attack?'. It seems like the world is starting to see that increased security measures are not just a matter of protecting data, but in protecting data, we are protecting the very infrastructure of our business.

There are many ways organizations can protect their business from cyber-attacks. The article is from a PrivacyEnd post which outlines several measures including; updated software, improved technologies, skilled employees and pre-planned precautionary measures.

I have extracted the five suggestions from the PrivacyEnd article that I wish to explore in more depth to provide you with recommendations and tips for enhancing your organization's data security.

❖ **Limit Data Access**

Most of the organizations give privileged access to their sensitive data to a number of employees and insiders. Think about who in your organization has access to sensitive customer data? Can you identify everyone's access rights? Most company executives are unaware of the details about individual employees who have access to data and why they access it. This is a huge risk to data loss, theft and hacking.

This means it is necessary for businesses to limit the data access. Organization's should determine what an employee needs access to and ensure they have access to only what they need. Not anything else. These all limitations could help organizations to manage their data more efficiently and ensure it is being safeguarded from theft or loss.

According to Dircks, Bomgar CEO,

With the continuation of high-profile data breaches, many of which were caused by compromised privileged access and credentials, it’s crucial that organizations control, manage, and monitor privileged access to their networks to mitigate that risk. The findings of this report tell us that many companies can’t adequately manage the risk related to privileged access. Insider breaches, whether malicious or

unintentional, have the potential to go undetected for weeks, months, or even years – causing devastating damage to a company.

❖ **Identify Sensitive Data**

For companies, it is really important to be aware of where their most important data and sensitive business information lies. This will ensure you have the right information and allocate more resources to protecting your most sensitive and crucial assets.

Although sensitive business data is only probably around 5-10% of your total business data, a data compromise involving sensitive or personal data could result in an immense loss of reputation and revenue to a company. If we go back to access management and rights, we should be putting more strict measures on sensitive data over other business data.

❖ **Pre-Planned Data Security Policy**

When looking at the operations and processes needed to mitigate a cyber-attack, an important step is to prepare a list of security measures and data security policies. This sort of plan by an organization could help significantly in critical situation and times of incident response. Through policies, you can immediately react in order to prevent extreme impacts of a cyber-attack.

As with access management and rights, employee access could be identified easily and you would remain aware of which users in your organization could have potentially been breached. It's important to remember that a policy and process plan is only as good as it's last revision. Technology, industry regulation and best practice is always changing. Someone therefore needs to own this policy and process guide and always look at new ways of updating it to keep it relevant.

❖ **Strong and Different Passwords for Every Department**

Sensitive data in an organization should be locked away with strong passwords. Making stronger passwords is necessary for fighting a number of password hacking tools that are easy to get on the market. Try ensuring that there are a combination of different characters including alphabets, numbers, symbols and other capital letters.

Additionally, using the same passwords for different programs and access is also a risk. Once your password is cracked, a hacker will try the same password on all major accounts you own.

Therefore, organizations should keep unique passwords for all employees as well as the departments. This can be easily managed using a password manager tool and ensuring that all employees receive proper data security training and password tips.

Where possible, it is also advised that multi-factor authentication is used. Adding another step to a password login means another step that hackers need to crack, making the hack much more unlikely and difficult. Some good examples of multi-factor authentication include biometrics, push notifications to phones, smartcards and token authentication.

❖ **Regular Data Backup and Update**

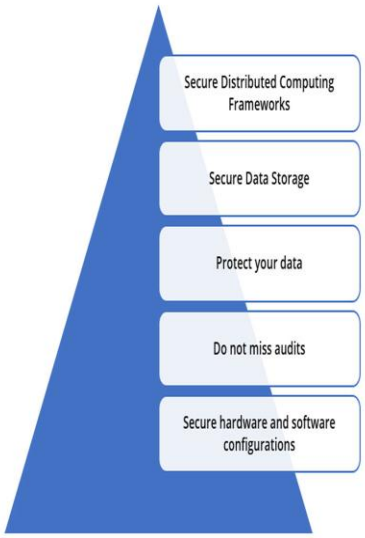
Last on the list of important data security measures is having regular security checks and data backups. For an unexpected attack or data breach, it is really helpful to have an organization back up their data. To have a successful business, you must keep a habit of automatic or manual data backup on a weekly or daily basis.

In addition, the data should be protected through updated software and efficient antivirus tools. However, to attain this, you must have progressive and efficient IT

department. Make sure you are hiring someone with the right skills who you can trust to do the job properly.

WHY ORGANIZATIONS SHOULD CARE ABOUT BIG DATA SECURITY?

Big data technology ingests large chunks of data, which lead involves significant risk to database security as containing such large volumes of critical data can result in a data breach. These data breaches may involve useful information such as credit card details, bank details, and various other personal information, a theft of which may cause devastating consequences. These data breaches may lead end users into distrusting their organizations. This highlights the need for more scalable big data tools, which will reduce these data thefts. The purpose of big data security is to build a firewall for unauthorized users, keep strong user-authentication, and ensure end-user training. Additionally, it aims at providing intrusion protection systems and intrusion detection systems, which operate at all data stages. The list below highlights ways that organizations can use with big data to resolve issues regarding security:



1. Secure Distributed Computing Frameworks

Distributed computing frameworks such as Spark, Hadoop, MPI have a considerable risk of data leakage. Additionally, they have a chance of being associated with untrusted mappers. Cloud Security Alliance (CSA) recommends companies to use authentication methods and establish trust. Furthermore, de-identification must be inculcated to ensure privacy constraints are met. Then, organizations must validate access to files and ensure that sensitive data is not leaked by any means.

2. Secure Data Storage

Data must be stored in a secure way to enhance big data security. To secure data storage, a technique called secure untrusted data repository (SUNDR) must be employed to monitor unauthorized alterations from third party agents.

3. Protect your data

While organizations assimilate large chunks of data to improve their services, collecting data is a difficult and expensive task. To secure your data, organizations must use firewall security, intrusion detection and prevention tools, scanning tools, and demand validation for all access to data.

4. Do not miss audits

Auditing is a must with big data security, and it is vital to maintain the audit data separately for future reference. Post any attack, organizations must conduct a complete audit to check whether operations are working fine. Technologies like Apache Oozie can help to understand big data clusters better.

5. Secure hardware and software configurations

Hardware or software malfunction is one of the important causes of data loss in any organization. Hence, it is essential that organizations manage hardware and

software configurations by ensuring it is updated regularly.
Preventing data breaches is one of the processes that organizations are inculcating in their culture with scalable big data analytical tools. Organizations must secure their big data platforms from threats to serve their business without interruption for years.

Nine important elements to cover in adata security policy

1. **EnsuringData Security Accountability**– A company needs to ensure that its IT staff, workforce and management are aware of their responsibilities and what is expected of them. The various types of data should be classified so that both workers and management understand the differences. By categorizing data, employees are aware of how to handle each type and which types they are allowed to distribute. Important classes to include in the policy are:

- ❖ Confidential data
- ❖ Data that is meant to be sent internally within the company
- ❖ General data
- ❖ Data that is meant to be sent outside the company

2. Policies that Govern Network Services – This section of the data security policy dictates how the company should handle issues such as remote access and the management and configuration of IP addresses. It also covers the security of components like routers and switches. This category is also where policies regarding the detection of network intrusion should be defined.

3. Scanning for Vulnerabilities–It is important to find any vulnerabilities in a company's IT infrastructure before hackers do. Since hackers will scan for vulnerabilities the minute they are discovered, a company should have a routine in place for checking its own networks regularly.

4. Managing Patches – Implementing code to eliminate vulnerabilities can help to protect against threats. How and when patches are to be implemented in the system should be a part of the data security policy.

5. System Data Security Policies – The security configuration of all essential servers and operating systems is a critical piece of the data security policy. Rules regarding servers that run on the company's networks as well as the management of accounts and passwords must be clearly defined. Firewall, database and antivirus policies also fall under this heading.

6. The Response to Incidents– If a security breach occurs, it's important to have appropriate measures for handling it already in place. This includes the evaluation and reporting of the incident as well as how to solve the problems leading to it to prevent the issue from reoccurring.

7. Acceptable Use – Employees should be provided with precise definitions of what constitutes acceptable use. Additionally, it is a good idea to have them sign an acceptable use policy so that the company can pursue disciplinary action if necessary.

8. Monitoring Compliance– The use of audits is a good way to ensure that the company's staff and management are complying with the various elements of a data security policy. These audits should be performed on a regular schedule.

9. Account Monitoring and Control – Keeping track of who is accessing what is an important component of a data security policy. Some of the most common sources of digital compromises are legitimate but inactive user accounts. This can occur when a staff member has been fired or laid off but his or her account not been terminated. If the employee is disgruntled, the ability to still access the organization's assets can be highly damaging. The security policy should designate specific IT team members to monitor and control user accounts carefully, which would prevent this illegal activity from occurring.

There are many more important categories that a security policy should include, such as data and network segmentation, identity and access management, and more. It should also address the organizations' entire security posture, monitoring all activity across every IT asset looking for abnormal and/or suspicious activity and activity patterns.

Once the policy is instituted and implemented across the enterprise, it should be reviewed at least twice a year to bring it current. Review should be triggered when significant upgrades are made to a company's network infrastructure. Organizations that are serious about preventing cyber crime must also consider the important link between data security and data privacy and create the custom policy that will safeguard the data they're entrusted with is used properly, legitimately and with the confidence that company and customer data is kept safe and secure.

Importance of IT Security in Business

IT security is important for any business. Organizations don't like to talk about it, but security breaches are constantly happening to businesses, sometimes multiple times a month. Cybercriminals are constantly looking to hack businesses and many succeed. A good security system protecting IT for businesses is the best defense a company can have against these cybersecurity threats. The importance of cybersecurity for a business is not just about their information being protected but also the information of their employees and customers. Companies have a lot of data and information on their systems. This fact adds to the importance of security, whether it is data security, information security or cybersecurity in general.

Importance of Cybersecurity Awareness

There are many benefits of cybersecurity for a business. When it comes to cybersecurity, it is important for a company to not only train and inform the higher-ups but every employee, of the benefits of cybersecurity. When a company trains all of its employees about the benefits of cybersecurity, the company itself has less exposure to cybersecurity risks in the first place. A company will save money with cyber-related loss and severity of cybersecurity incidents when they offer their employees proper cybersecurity training. Another benefit of training employees is the time saved. When a company has fewer cybersecurity threats, the employees of that company will spend less time tracking down the treat, fixing it and possibly having to redo any affected work. When employees are properly trained, when it comes to cybersecurity, they develop a more positive company culture with regards to cyber and information security.

Cybersecurity Solutions

There are many ways to ensure a business is practicing effective cybersecurity. One of the biggest ways is to train and educate employees of the significance of cybersecurity and the benefits of keeping the company secure. Another tool companies use is cybersecurity services provided by a reliable cybersecurity company. A few of those reliable companies include:

- Herjavec Group
- Raytheon Cyber
- IBM Security
- Thycotic
- Digital Defense
- Palo Alto Networks

Cybersecurity is important for any organization that has critical data and information they can not afford to lose. When it comes to hackers, many companies are defenseless against attacks. The reason for this is in part due to lack of employee knowledge and lack of proper cybersecurity service. Companies need to protect themselves against attacks and education can help a great deal. When employees are aware of the importance of cybersecurity, they will do their part to achieve security for their company.

Data Protection Act 2018 - Criminal Offences

Introduction

The Data Protection Act 2018 (DPA 2018) came into force on 25 May 2018, replacing the Data Protection Act 1998. The DPA 2018 brought the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) into UK Law.

What is the GDPR?

GDPR is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). It is brought in to UK Law by means of Part 2 of the DPA 2018.

What is the LED?

Part 3 of the DPA 2018 transposes the EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law and sets out the requirements for the processing of personal data for criminal 'law enforcement purposes'.

What is personal data?

Personal data is any information relating to an identified or identifiable living individual. An identifying characteristic could include a name, ID number or location data. You should treat such information as personal data even if it can only be potentially linked to a living individual.

Offences under the DPA 2018

Section 119: Obstructing the Commissioner in inspecting personal data to discharge an international obligation

Section 119 is described as a 'future-proofed' version of s.54A DPA 1998. It is a provision that criminalises obstructing the ICO's inspection of European information systems. The Commissioner may inspect personal data where the inspection is necessary in order to discharge an international obligation of the United Kingdom, subject to the restriction in subsection (2). Section 119 (6) states that it is an offence (a)intentionally to obstruct a person exercising the power under subsection (1), or (b)to fail without reasonable excuse to give a person exercising that power any assistance the person may reasonably require.

Section 132: Prohibition placed upon the Commissioner, or the Commissioner's staff against disclosing information obtained in the course of their role (which is not available to the public)

Section 132 replaces section 59 DPA 1998 and criminalises action by former or current ICO staff who disclose data obtained during the course of their duties. Section 132 (2) clarifies the circumstances in which disclosure – with lawful authority – may be made. Section 132 (3) however confirms that it is an offence for a person knowingly or recklessly to disclose information in contravention of subsection (1).

Section 144: False statement made in response to an information notice
It is an offence for a person, in response to information notice from the Commissioner, to make or recklessly make, a statement which they know to be false in a material respect.

Section 148: Destroying or falsifying information and documents etc
Under Section 148 (2) (a) it is an offence for a person to destroy or otherwise dispose of, conceal, block or (where relevant) falsify all or part of the information, document, equipment or material. Section 148 (2) (b) makes to cause or permit the actions set pout in the previous subsection.

Section 170: Unlawful obtaining etc of personal data
Section 170 of the Act builds on section 55 DPA 1998 which criminalised knowingly or recklessly obtaining, disclosing or procuring personal data without the consent of the data controller, and the sale or offering for sale of that data. The provision was most typically/commonly used to prosecute those who had accessed healthcare and financial records without a legitimate reason. Section 170 adds the offence of knowingly or recklessly retaining personal data (which may have been lawfully obtained) without the consent of the data controller. There are some exceptions: for example where such obtaining, disclosing, procuring or retaining was necessary for the purposes of preventing or detecting crime. Section 170 (2) and (3) set out the defences to Section 170 (1).

Section 171: Re-identification of de-identified personal data
Section 171 - a new offence - criminalises the re-identification of personal data that has been 'de-identified' (de-identification being a process - such as redactions - to remove/conceal personal data). Section (5) states that it is an offence for a person knowingly or recklessly to process personal data that is information that has been re-identified. Sections 171 (3) and (4) set out the defences to Section 171 (1) – for example, the re-identification was necessary for the purposes of preventing or detecting crime. Sections 171 (6) and (7) set out the defences to Section 171 (5).

Section 173: Alteration etc of personal data to prevent disclosure to data subject
(also features in criminal offences list below)

Section 173 relates to the processing of requests for data from individuals for their personal data. Section 173 (3) makes it a criminal offence for organisations (persons listed in Section 173 (4)) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure. It builds on an offence under the Freedom of Information Act 2000. Possible defences to an offence under section 173 (3) are set out in Section 173 (5).

Section 184: Prohibition of requirement to produce relevant records
Section 184 (1) makes it an offence for a person to require another to provide them with or give them access to a relevant record linked to the employment, continued employment of one of their employees or a contract for the provisions of services to them. Section 184 (2) makes it an offence for a person to require another to provide them with or access to a relevant record if

the requestor is involved in the provision of goods, facilities or services to the public or the requirement is a condition of providing or offering to provide goods, facilities or services to the other person or a third party. Section 184 (3) details the possible defences to offences under subsection 184 (1) or (2).

Schedule 15, Paragraph 15. Powers of Entry and Inspection
It is an offence under paragraph 15 (1) for a person to intentionally obstruct a person in the execution of a warrant issued under this Schedule or to fail without reasonable excuse to give a person executing the warrant such assistance as may be required. Under paragraph 15 (2) it is an offence for a person to make a statement in response to a requirement under paragraph 5(2(c) or (d) or 3(c) or (d) which the person knows to be false in a material respect or recklessly make such a statement.

There are no custodial sentences in respect of offences under DPA 2018 and no powers of arrest; all offences are punishable only by a fine.

Schedule 15 – Powers of entry and inspection, sets out the circumstances in which the Information Commissioner may apply for a search warrant.

The DPA 2018 removed Section 77 (power to alter penalty for unlawfully obtaining etc personal data) of the Criminal Justice and Immigration Act 2008.

Notification Offence

Under the DPA 2018, organisations that determine the purpose for which personal data is processed (controllers) must pay the ICO a data protection fee unless they are exempt. The new data protection fee replaces the requirement to 'notify' (or register), which was in the DPA 1998. The Information Commissioner has the power to enforce the DPA 2018 and to serve monetary penalties on those who refuse to pay their data protection fee.

Right of data subjects

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Guidance on the CPS' obligations in respect of these rights can be found here: Data protection and the CPS and Privacy Notice.

Changes to Criminal Offences under the Data Protection Act 2018

The data protection regime underwent a monumental change in recent weeks, with the enactment of GDPR and the Data Protection Act ('DPA') 2018. Perhaps overlooked are the changes which was made to criminal offences under the Act. This article will provide an overview of the key changes, of which criminal practitioners should be aware.

Firstly, some jargon busting. A 'data controller' under the Act is a person who (alone or with others) decides the purposes for which and the way personal data is processed. A 'data subject' is a person whose data is stored. A 'subject access request' is a request by an individual to an organization to discover the information which is held about them.

The offence of unlawfully obtaining, or disclosing, personal data without the consent of the data controller (formerly s.55 DPA 1998) is a common feature of many prosecutions brought by the Information Commissioner's Office ('ICO'). This

offence is applicable in a variety of situations. A claims management company trading personal data for a fee, without the consent of a data controller, is guilty of this offence. Equally, a receptionist in a medical practice who uses the information in the practice's database to look up family and friends out of curiosity would also be guilty of this offence.

This offence has now been amended, and can be found at s.170 DPA 2018. There is a new clause in which it is a criminal offence to retain personal data without the consent of the data controller. This would cover a situation where data was provided through lawful means, then retained beyond the time consented to by the data controller. This aspect of the offence, therefore, has a broad remit.

The offence under s.170 DPA 1998 remains punishable only by way of a fine. In the previous legislation, there was a caveat which permitted the Secretary of State to alter the penalty to a custodial sentence (s.77 Criminal Justice and Immigration Act 2008). This was never used in the lifetime of the old Act. There is no provision for such a power in the new legislation. It remains the case that there are no formal sentencing guidelines for this offence.

Punishment for an offence under s.170 DPA 2018 is now confined to a financial penalty. That being so, it is conceivable to consider that, if the offending behaviour is sophisticated and/or longstanding, and causes a significant degree of harm, a prosecuting authority may take the view that charging an offence that only allows for a financial penalty would not suitably cover the criminality. There are other offences that could potentially be charged in such cases, such as fraud or computer misuse act offences and these may now be charged more frequently. It would not be wise to reassure a client that they will avoid an imprisonable offence if they have committed a data breach offence, as their prosecution may simply fall under a different guise.

A new offence created under DPA 2018 is the re-identification of de-identified personal data (s.171 DPA 2018). If personal data has been anonymised by a data controller, and the document is later amended to reveal the data without the consent of the data controller. This may have broader implications in the investigation of crime, where documents are commonly redacted and disclosed. It is possible to use software to remove the redaction on documents. To use such software, without consent, would be a criminal offence.

It remains a criminal offence to require an individual to exercise their subject access rights to gain their personal information in relation to their employment, a contract for services or the provision of goods and services (s.184 DPA 2018). It is common practice for employers to conduct their own pre-employment checks e.g. a Disclosure Barring Service ('DBS') check. If a data subject were to make the request (a subject access request) they would receive more information than would be included in a DBS check. The response to a subject access request would also include 'spent' convictions. It is a criminal offence for an employer to insist on receiving enhanced information in this way. This offence has been amended, to encompass an employer making the request recklessly.

Other criminal offences to be aware of under DPA 2018 are as follows:

119 DPA 2018- obstructing the Commissioner in inspecting personal data to discharge an international obligation.
131 DPA 2018- making a disclosure prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.

132 DPA 2018- prohibition placed upon the Commissioner, or the Commissioner's staff against disclosing information obtained in the course of their role (which is not available to the public).
144 DPA 2018- false statement made in response to an information notice.
173 DPA 2018- alteration of personal data etc to prevent disclosure to data subject.
Para 15, Schedule 15 DPA 2018- intentional obstruction of a warrant, or failure without reasonable excuse to assist in the execution of a warrant.
Many offences under the new DPA are now recordable, which was not a feature of the old Act. It may be that this has a deterrent effect on individuals who routinely exchange personal data without consent.

The latest raft of legislation has put the use which can be made of personal data into even sharper focus than before. It may be that offences arising from the DPA 2018 become a more prominent feature within our courts.

Security of DBMS

Security Policies:
A security policy is a collection of standards, policies, and procedures created to guarantee the security of a system and ensure auditing and compliance. The security audit process starts by identifying the security vulnerabilities in the organization's information system infrastructure and identifying measures to protect the system and data against those vulnerabilities.

Security Vulnerabilities:
Security vulnerability is a weakness in a system component that could be exploited to allow unauthorized access or cause service disruptions. The nature of such vulnerabilities could be of multiple types: technical (such as a flaw in the operating system or Web browser), managerial (for example, not educating users about critical security issues), cultural (hiding passwords under the keyboard or not shredding confidential reports), procedural (not requiring complex passwords or not checking user IDs), and so on. Whatever the case, when a security vulnerability is left unchecked, it could become a security threat. A security threat is an imminent security violation that could occur at any time due to unchecked security vulnerability.

A security breach occurs when a security threat is exploited to negatively affect the integrity, confidentiality, or availability of the system. Security breaches can yield a database whose integrity is either preserved or corrupted:

• Preserved: Action is required to avoid the repetition of similar security problems, but data recovery may not be necessary. As a matter of fact, most security violations are produced by unauthorized and unnoticed access for information purposes, but such snooping does not disrupt the database.

• Corrupted: Action is required to avoid the repetition of similar security problems, and the database must be recovered to a consistent state. Corrupting security breaches include database access by computer viruses and by hackers whose actions are intended to destroy or alter data.

Database Security:
Database security refers to the use of the DBMS features and other related measures to comply with the security requirements of the organization. From the DBA's point of view, security measures should be implemented to protect the DBMS against service degradation and the database against loss, corruption, or mishandling.

To protect the DBMS against service degradation there are certain minimum recommended security safeguards. For example:

• Change default system passwords.
• Change default installation paths.
• Apply the latest patches.
• Secure installation folders with proper access rights.
• Make sure only required services are running.
• Set up auditing logs.
• Set up session logging.
• Require session encryption.

Protecting the data in the database is a function of authorization management. Authorization management defines procedures to protect and guarantee database security and integrity. Those procedures include, but are not limited to, user access management, view definition, DBMS access control, and DBMS usage monitoring.

• **User access management**: This function is designed to limit access to the database and likely includes at least the following procedures:

• **Define each user to the database**: This is achieved at the operating system level and at the DBMS level. At the operating system level, the DBA can request the creation of a logon user ID that allows the end user to log on to the computer system. At the DBMS level, the DBA can either create a different user ID or employ the same user ID to authorize the end user to access the DBMS.

• **Assign passwords to each user:** This, too, can be done at both operating system and DBMS levels. The database passwords can be assigned with predetermined expiration dates. The use of expiration dates enables the DBA to screen end users periodically and to remind users to change their passwords periodically, thus making unauthorized access less probable.

• **Define user groups**: Classifying users into user groups according to common access needs facilitates the DBA's job of controlling and managing the access privileges of individual users. Also, the DBA can use database roles and resource limits to minimize the impact of rogue users in the system.

• **Assign access privileges**: The DBA assigns access privileges or access rights to specific users to access specified databases. An access privilege describes the type of authorized access. For example, access rights may be limited to read-only, or the authorized access might include READ, WRITE, and DELETE privileges. Access privileges in relational databases are assigned through SQL GRANT and REVOKE commands.

• **Control physical Access**: Physical security can prevent unauthorized users from directly accessing the DBMS installation and facilities. Some common physical security practices found in large database installations include secured entrances, password-protected workstations, electronic personnel badges, closed-circuit video, voice recognition, and biometric technology.

• **View definition**: The DBA must define data views to protect and control the scope of the data that are accessible to an authorized user. The DBMS must provide the tools that allow the definition of views that are composed of one or more tables and the assignment of access rightsto a user or a group of users. The SQL command CREATE VIEW is used in relational databases to define views.

• **DBMS access control:** Database access can be controlled by placing limits on the use of DBMS query and reporting tools. The DBA must make sure that those tools are used properly and only by authorized personnel.

• **DBMS usage monitoring**: The DBA must also audit the use of the data in the database. Several DBMS packages contain features that allow the creation of an audit log, which automatically records a brief description of the database operations performed by all users. Such audit trails enable the DBA to pinpoint access violations.

References:

[1] *https://www.techopedia.com/definition/26464/data-security*
[2] https://www.techopedia.com/definition/13602/data-masking
[3] https://www.techopedia.com/definition/25054/health-care-data-encryption
[4] https://www.techopedia.com/definition/15337/electronic-health-record-ehr
[5] https://www.techopedia.com/definition/15337/electronic-health-record-ehr
[6] https://www.techopedia.com/definition/3805/hacker
[7] https://www.techopedia.com/definition/4275/exploit
[8] https://www.techopedia.com/definition/5/information-assurance-ia
[9] https://www.techopedia.com/definition/60/hacking-tool
[10] https://www.techopedia.com/definition/16089/ethical-hacker
[11] https://www.techopedia.com/definition/13656/mode-of-attack
[12] https://www.globalsign.com/en/blog/5-ways-to-enhance-data-security/
[13] https://www.allerin.com/blog/5-ways-an-organization-can-manage-its-big-data-security
[14]https://www.securitymagazine.com/articles/87113-important-elements-to-corporate-data-security-policies-that-protect-data-privacy
[15] https://www.techfunnel.com/information-technology/role-cyber-security-organization/
[16] https://www.cps.gov.uk/legal-guidance/data-protection-act-2018-criminal-offences
[17] https://www.lincolnhousechambers.com/changes-criminal-offences-data-protection-act-2018
[18] http://www.myreadingroom.co.in/notes-and-studymaterial/65-dbms/573-security-of-dbms.html

Syed Jamaluddin Ahmad, achieved Bachelor of Science in Computer Science and Engineering (BCSE) from Dhaka International University, Masters of Science in Computing Science Associates with research: Telecommunication Engineering from Athabasca University, Alberta, Canada and IT-Pro of Diploma from Global Business College, Munich, Germany. Presently Working as an Assistant Professor and Head of the Department, Computer Science and Engineering, Shanto-Mariam University of Creative Technology, Dhaka, Bangladesh. Formerly, was head of the Department of Computer Science & Engineering, University of South Asia from 2012-2014, also Lecturer and Assistant Professor at Dhaka International University from 2005-2007 and 2011-2012 respectively and was a lecturer at Loyalist College, Canada, was Assistant Professor at American International University, Fareast International University, Royal University, Southeast University and Many more. He has **alrea**dy 15th international publications, 12th seminar papers, and conference articles. He is also a founder member of a famous IT institute named Arcadia IT (www.arcadia-it.com). Achieved Chancellor's Gold Crest in 2010 for M.Sc. in Canada and Outstanding result in the year of 2005. and obtained "President Gold Medal" for B.Sc.(Hon's). Best conductor award in Germany for IT relevant works. Membership of "The NewYork International Thesis Justification Institute, USA, British Council Language Club, National Debate Club, Dhaka,

English Language Club and DIU . Developed projects: Mail Server, Web Server, Proxy Server, DNS(Primary, Secondary, Sub, Virtual DNS), FTP Server, Samba Server, Virtual Web Server, Web mail Server, DHCP Server, Dial in Server, Simulation on GAMBLING GAME Using C/C++, Inventory System Project, Single Server Queuing System Project, Multi Server Queuing System Project,

Random walk Simulation Project, Pure Pursuit Project (Air Scheduling), Cricket Management Project, Daily Life Management Project, Many Little Projects Using Graphics on C/C++, Corporate Network With Firewall Configure OS:LINUX (REDHAT) Library Management Project Using Visual Basic, Cyber View Network System:Tools:Php OS: Windows Xp Back-end: My SQL Server, Online Shopping: Tools: Php, HTML, XML. OS:Windows Xp, Back-end: My SQL and Cyber Security" Activities-'Nirapad Cyber Jogat, Atai hok ajker shapoth'-To increase the awareness about the laws, 2006 (2013 amendment) of Information and Communication and attended Workshop on LINUX Authentication"-Lead by- Prof. Andrew Hall, Dean, Sorbon University, France, Organized By- Athabasca University, CANADA, April, 2009. His areas of interest include Data Mining, Big Data Management, Telecommunications, Network Security, WiFi,

Wimax, 3g, 4g network, UNIX, LINUX Network Security,Programming Language(C/C++ or JAVA), Database (Oracle), Algorithm Design, Graphics Design & Image Processing and Algorithm Design.

Roksana Khandoker, achieved Bachelor of Science in Computer Science and Engineering (BCSE) from United International University, Masters of Science in Computer Science and Engineering from University of South Asia. Presently Working as a Senior Lecturer, Computer Science and Engineering, University of South Asia, Dhaka, Bangladesh. Formerly, was also a lecturer at different poly-technique institutes. She has 4th international journals and attended different international and national conferences. She is the Chairman of the famous IT institute named Arcadia IT and Chairman of Brighton International Alliance. Her areas of interest include Data Mining, Big Data Management, Telecommunications, Network Security, WiFi, Wimax, 3g and 4g network.

Tasnim Niger, achieved Bachelor of Science in Computer Science and Engineering (CSE) from International Islamic University Chittagong, Masters in Information Technology (MIT) fromInstitute of Information Technology - University of Dhaka. Currently pursuingPhD in Islamic University of Technology (IUT).Presently working as a Lecturer of Computer Science and Engineering of Shanto-Mariam University of Creative Technology, Dhaka, Bangladesh. Formerly, was Lecturer of City University, Dhaka from 2013-2014. She is a Life member of Dhaka University Alumni Association- LM# 7547. Her areas of interest include Artificial Intelligence, Machine Learning, Data Mining, Big Data Management, Data Security, Human Computer Interaction,Programming Language(C/C++ or JAVA, Python), Database (Oracle), Image Processing etc.

Farzana Nawrin achieved Bachelor of Science in Computer Science and Engineering (BCSE) from Dhaka City College under National University, Masters of Science in Computer Science from Jahangirnagar University. She achieved 1st class 1st both B.Sc. and M.Sc. degree. Presently working as a lecturer, Computer Science and Engineering department, Shanto-Mariam University of Creative Technology, Dhaka, Bangladesh. Formerly, was also a lecturer of Computer Science and Engineering department of Dhaka City College under National University. She has done two thesis about network security in her B.Sc. and M.Sc. level. She has three international journals. She was also attended many national workshop. She has got special training from Bangladesh Institute of Design and Development(BIDD). She has special certification in CCNA and CompTIA A+. Her areas of interest include Network Security, Telecommunication, System analysis, Automata Design, Routing and Switching, Design and Analysis Compiler, Wifi,Wimax,3g and 4g Network.