What to do after data is breached and how to restore data – A Review on Cyber Security

Dr. Manish Pandey[1], **Rakesh Kumar**[2]
[1]*Professor, Himalayan University, Itanagar, Arunachal Pradesh*
[2]*Assistant Professor, Department of Computer Application, Tula's Institute, Dehradun*

Abstract
The current world is run by technology and network connections, it is crucial to know what cyber security is, it should be understood to be able to use it effectively. If there is no security to protect it, systems, important files, data, and other important virtual things are at risk. Every company, whether it is an IT firm or not, must be protected equally. With the advancement of the new technology, the attackers do not lag behind in terms of cyber security technology. The hackers are using improved hacking techniques and are targeting the weak points of many businesses. Cyber security is critical because the military, government, and other organizations rely on it. Financial, medical, and corporate organizations amass, practice, and store unprecedented amounts of data on PCs and other devices. A significant portion of that data may contain sensitive information, such as financial information or intellectual property, personal information, or other types of data for which unauthorized access or acquaintance could result in negative consequences. With the help of proper tools as well as management, we can prevent our data from getting breached. This research paper is made using the APA method. All in all, cybersecurity is quite a serious topic to have a discussion about which is why this paper is written in order to give an insight to what we can do if our data is breached.

1. INTRODUCTION

What exactly is data breaching?

Data Breaching is a type of cyber incident which results in losing your data. Likewise, 'cyber incident' is the actions taken through the use of an information system or network that have an actual or potential negative impact on an information system, network, and/or the information contained therein.

A security breach occurs when an unauthorized user penetrates or circumvents cybersecurity measures to gain access to a system's protected areas. The perpetrator could be a human, such as a cyber hacker, or a self-directing program, such as a virus or other type of malware.

Security breaches can be the result of either intentional or unintentional actions. An intentional security breach is usually motivated by one of two factors. The attacker's goal is usually to gain access to secure information (resulting in a data breach), to use computing resources for their own purposes (as in cryptojacking attacks), or to crash the network itself for personal or political reasons. As terrifying as these attacks can be, they are often easier to detect and plan for than accidental breaches caused by a combination of error and negligence.

Types of data breaches

Although the terms are frequently used interchangeably, a security breach and a data breach are not synonymous. A security breach is a breach of cybersecurity controls, but it does not always imply that private or confidential data has been compromised. When secure information is accessed by an unauthorized user or released into an untrusted environment, this is referred to as a "data breach."

There are seven distinct categories:

1. **Hacking Intrusions**

   This category includes a wide range of techniques used by cybercriminals to gain access to secure data, such as phishing scams, brute force access attempts, ransomware, and various viruses/malware.

2. **Insider Threat**

   Insider threat is a particularly dangerous type of data breach in which an employee (or vendor) uses their knowledge of security controls to access and compromise data, usually for financial gain.

3. **Data on the Move**

   Portable storage devices, such as laptop hard drives, backup tapes, and flash drives, are useful for physically transporting data from one location to another, but they can be lost or damaged in transit.

4. **Physical Theft**

   While most businesses keep their IT networks safe behind firewalls and cyber security software, they must also deal with the possibility of someone walking out the front door with a company laptop containing proprietary, and potentially sensitive, information. A thief could also use social engineering techniques to gain access to a secure location and download data onto a portable drive.

5. **Human Error**

   Unfortunately, mistakes do occur. They are quite common when it comes to cyber security and data handling.

6. **Accidental Internet Exposure**

   Most organizations understand that exposing data to the public internet increases the risk of exposure and unauthorized access significantly. This was less of an issue when data was primarily stored on-premises servers and accessed via LAN connections, but the rise of cloud computing has forced businesses to take much more proactive measures to protect data accessed via the internet. When data is exposed to the public internet, it increases the possibility of accidental data leakage or "man in the middle" cyberattacks.

7. **Unauthorized Access**

   Weak access controls, such as poorly monitored admin privileges or a lack of user segmentation, can lead to people handling and sharing data that they have no business handling. Without good access policies in place, organizations increase the likelihood of other types of security breaches occurring, eventually leading to costly data breaches.

What Are the Weaknesses?

In many ways, cybersecurity is an arms race between attackers and defenders. ICT systems are extremely complex, and attackers are constantly probing for flaws that can occur at multiple points. Defenders can often protect against weaknesses, but three are particularly difficult: inadvertent or intentional acts by system insiders; supply chain vulnerabilities, which can allow the insertion of malicious software or hardware during the acquisition process; and previously unknown, or zero-day, vulnerabilities with no established fix. Even when remedies for vulnerabilities are known, they may not be implemented in many cases due to budgetary or operational constraints.

What are the Impacts?

A successful attack can compromise the confidentiality, integrity, and availability of an ICT system and the information it handles. Cybertheft or cyberespionage can result in exfiltration of financial, proprietary, or personal information from which the attacker can benefit, often without the knowledge of the victim. Denial-of-service attacks can slow or prevent legitimate users from accessing a system. Botnet malware can give an attacker command of a system for use in cyber attacks on other systems. Attacks on industrial control systems can result in the destruction or disruption of the equipment they control, such as generators, pumps, and centrifuges.

Most cyber attacks have limited consequences, but a successful attack on some components of critical infrastructure (CI), the majority of which is held by the private sector, could have significant consequences for national security, the economy, and individual citizens' livelihoods and safety. As a result, a rare successful attack with a high impact can be more dangerous than a common successful attack with a low impact. While it is widely acknowledged that cyber attacks can be costly to individuals and organizations, the economic consequences are difficult to quantify, and estimates of those consequences vary widely.

The annual cost of cybercrime to the global economy is frequently cited as $400 billion, with some observers arguing that costs are rising significantly, especially with the continued expansion of ICT infrastructure through the Internet of Things and other new and emerging platforms. The costs of cyberespionage are even more difficult to quantify, but are thought to be significant. Managing cyberattack risks typically entails (1) removing the threat source (e.g., by shutting down botnets or reducing incentives for cybercriminals); (2) addressing vulnerabilities by hardening ICT assets (e.g., by patching software and training employees); and (3) mitigating impacts by mitigating damage and restoring functions (e.g., by having backup resources available for continuity of operations in response to an attack). The optimal level of risk reduction will differ between industries and organizations. Customers may expect a lower level of cyber security from an entertainment company than from a bank, hospital, or government agency, for example.

2. PREPARING FOR A SECURITY BREACH

When it comes to recovering from a security breach, preparation is essential. If you don't have the right tools, you might not even be able to detect a security breach, let alone contain and eliminate it.

Here are some key preparations to help protect your organization from a security incident. The better prepared you are for an attack, the easier it will be to respond quickly. This, in turn, helps to mitigate the consequences of a cyber security breach.

Identifying your IT Assets

How can you protect your network if you have no idea what's on it? A complete audit of your network's IT assets is required if you want to account for all of the resources you need to protect—and possibly replicate as part of your recovery plan.

Integrate an Intrusion Detection System

The ability to detect a breach is critical for ensuring a quick response that minimizes damage and facilitates recovery and risk mitigation. Intrusion detection systems (IDSs) assist you in detecting security breaches so that you can respond to them as soon as possible. Intrusion prevention systems (IPSs) go a step further by automatically initiating network breach response measures that aid in the immediate containment of the attack. SIEM (security information and event management) systems can help gather information about a network hacking attempt in order to reveal the attack methodology, which is useful for preventing future attacks.

Make an Incident Response Strategy.

An incident response plan (IRP) is a document that outlines what each individual in the organization must do in the event of a network breach. Having an IRP in place enables employees to respond to network hacks more quickly and consistently, allowing the breach to be contained and eliminated more quickly. Setting up an incident response plan entails distributing the plan to all employees in the organization and then ensuring that they understand and can meet the expectations outlined in the IRP document. This may necessitate additional training sessions or meetings to go over the contents of the plan and explain how to use specific tools required to detect, contain, and eliminate a network breach.

Backup Your Information

Before an attack, it is critical to create a remote data backup of your organization's most critical information so that local files can be restored in the event of a network breach. This aids in the prevention of data loss caused by breaches that damage or encrypt locally stored files. It is also an essential component of a disaster recovery (DR) plan. Naturally, setting up the backup necessitates categorizing all of the organization's data so that the most critical information can be preserved in an emergency. Attempting to copy everything results in backup bloat, which slows down data copying and adds unnecessary costs (because of the extra storage needed to hold everything vs only needing to budget for mission-critical data).

Perform Regular Penetration Testing

Penetration tests are an important risk mitigation tool because they identify vulnerabilities in your security preparations and allow you to fix them before a breach occurs. A penetration test (also known as a "pen test") is a deliberate attempt by cybersecurity experts to breach your cybersecurity architecture. This assists in identifying potential network exploits, which you can then fix to prevent attackers from using them in a "zero day" attack. These tests should be performed on a regular basis, especially after major changes to your organization's software or IT hardware.

Form an Incident Response Team (IRT)

While having an incident response plan is beneficial, having the right people with the right skills and experience to handle your response to a security breach is equally important. An incident response team, whether drawn from internal IT staff or a third-party cyber security staffing provider, can help ensure that your IRP runs as smoothly as possible. Your IRT personnel will gather, analyze, and act on security incident information. Because they may have to deal with incidents other than data or network breaches, some organizations refer to this as a computer security incident response team (CSIRT).

3. HOW TO RESPOND TO A SECURITY BREACH

When a security breach occurs, organizations must have a clear plan of action. In these situations, the incident response plan should be the guiding light. Ideally, the plan will have been widely distributed throughout the organization to ensure that everyone understands their roles and responsibilities in the event of a cyber security incident.

Phase One of Breach Recovery: Attack Prevention

The first step toward recovery was recognizing that there was a breach at all. The sooner you detect a breach, the better off your company will be. This is because it will take time for any attackers to breach the first system they compromise in order to gain access to the rest of your network.

The second step is to contain the breach, which means cutting off the attacker's access by isolating the compromised system(s) or revoking the user account's access privileges.

The third step is to eliminate the threat once it has been contained. Depending on the type of breach, the method of elimination may differ. To remove a ransomware threat, for example, all affected data storage media may need to be completely formatted (or even physically removed and replaced). The destroyed data can then be recovered from a remote backup (assuming one exists).

You can reduce the damage caused by a breach if you can identify, contain, and eliminate it before the attacker breaks out of the system that was initially compromised.

Only after the source of the attack has been removed can the recovery process begin.

Phase Two of breach recovery is to Investigate the attack method.

Knowing how the attack occurred is essential for preventing attackers from simply repeating the same attack strategy. Additionally, any affected systems should be investigated for signs of further compromise—the attacker may have left other malware on the system during their time of access.

Activity logs from the time of the breach should be saved for later forensic analysis. These logs can assist you in determining the source of the attack and preventing future attempts.

Phase Three of breach recovery is to notify those who may have been affected.

You should be able to determine which systems were compromised and what data, if any, was put at risk of being compromised during your investigation of the breach. You should notify any and all parties who may have been affected by the security breach as soon as possible.

According to the National Conference of State Legislatures, notification laws vary by state. As a result, the time limit for your company to notify customers, vendors, and others affected by a breach may differ. As a general rule, the sooner you can send a notification, the better.

Notification contact methods may differ, and it is often a good idea to send notifications via multiple channels whenever possible to ensure that those affected by a breach are notified. You could, for example, send out a mass email, regular mail, or automated phone calls to notify customers that they may have been affected.

Include the date of the breach, what types of files may have been compromised, and what steps the message recipient should take to protect themselves based on the type of data that was compromised in the email/mail/phone message.

Sending these types of notices is critical for preserving your company's reputation following a breach. Being prompt and honest, in addition to working to protect customers who may have been impacted by a breach, shows that you value your customers' data security. As a result, the inevitable backlash that follows a major data security breach is mitigated.

Authorities should be notified as soon as possible so that they can assist with the investigation (and to comply with certain security breach notification laws).

Phase Four of Breach Recovery: Restoring Network Assets

Individual assets that were compromised to your network can be restored in a variety of ways, depending on how you prepared for the security breach. In some cases, it may be possible to simply wipe or replace the affected IT assets' data storage drives and download any lost data from a backup.

In other cases, you may be able to activate entire cloud-based replicas of your network environment to quickly restore your company's network while you investigate the security breach.

Essentially, how you restore assets on your network will be determined by your business continuity (BC) and disaster recovery (DR) plans. A BC/DR plan should be created well in advance to create fail-safes so that if one of your assets is taken down, you can keep your business running.

For example, if you have a remote, cloud-based replica of your primary production environment ready to go at any time, you might want to activate it while your primary production environment is taken offline for more extensive maintenance.

When restoring assets, keep track of which assets have been removed and which are supposed to be on your network based on your most recent asset identification efforts. This way, you can be certain that you haven't overlooked anything—and that no surprises have been left on your network.

Phase Five of Breach Recovery: Getting Ready for the Next Attack

After you've recovered from the attack by following your BC/DR plan, it's critical to prepare for the next attack. If you've been hit once, you're likely to be attacked again by the same group—or by others employing the same attack strategy.

This is where your investigation into the attack can be extremely useful. By investigating the attack method and determining how the attacker(s) gained access, you can identify and close the gaps in your cyber security that allowed the attack to occur. Regular Testing would also be a feasible option in order to prevent attacks. This can help to prevent future breaches.

In addition, researching your BC/DR plan implementation can teach you how to improve the plan in the future. Making these changes can help you respond faster to an attack and reduce the downtime and disruption that an attack can cause.

Legislative Actions and Proposals

Many bills addressing a variety of cyber security issues have been introduced since at least the 111th Congress:

Cybercrime Laws—updating criminal statutes and law enforcement authorities in the area of cyber security.

Data-Breach Notification—requires notification to victims and other responses following data breaches involving individuals' personal or financial information.

FISMA Reform is the process of updating the law to reflect changes in ICT and the threat landscape.

Information Sharing—improving access to classified and unclassified threat information for the private sector and removing barriers to sharing within the private sector and with the federal government.

Internet of Things—addresses a variety of cyber security issues arising from the proliferation of Internet-connected devices and objects (such as home appliances, automobiles, medical devices, factories, and infrastructure).

Privately Held CI—improving private sector CI protection from high-impact attacks.

Research and development—updating agency authorizations and strategic planning requirements.

Workforce—increase the size, skills, and readiness of the federal and private sector cyber security workforces.

4. CONCLUSION

It is a matter of when, not if, a security breach occurs, but an effective response can significantly reduce the impact. To accomplish this, you must plan ahead of time and implement appropriate detective measures – after all, you cannot respond to an incident if you are unaware that one has occurred.

Furthermore, just as you cannot put out a fire if you do not have fire extinguishers or sprinklers on hand, an effective cyber incident response is impossible if you are not prepared with the appropriate response measures. So, back up your data on a regular basis, implement remote wipe features, plan any other necessary technical measures and processes, and, most importantly, ensure that your employees understand what is expected of them.

Reference:

[1] IT Governance Green Paper: Cyber Incident Response Management (IT Governance Green Paper, 2021) https://www.compuquip.com/blog/how-to-recover-from-a-security-breach

[2] Cyber security Issues and Challenges: In Brief Eric A. Fischer

[3] Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime" (McAfee, June 2014), http://www.mcafee.com/us/resources/reports/rp-economic-impactcybercrime2.pdf?cid=BHP028; Cybersecurity Ventures, "Cybersecurity Market Report, Q2 2016," 2016,

[4] http://cybersecurityventures.com/cybersecurity-market-report/. For more information on the Internet of Things, see CRS Report R44227, The Internet of Things: Frequently Asked Questions, by Eric A. Fischer.

[5] Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace:

[6] Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," October 2011,

[7] https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report _fecie.pdf