IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

What to do after data is breached and how to restore data

Khushi Pokharel
+918929001077
khushi.pokharel@gmail.com
BCA IIIrd Year
Tula's Institute, Dehradun

Mr. Rakesh Kumar
Assistant Professor
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 in order to secure them. 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.

What exactly is data breaching?

A data breach is a type of cyber incident that results in the loss of your data. Similarly, a 'cyber incident' is defined as actions taken using an information system or network that have an actual or potential negative impact on an information system, network, and/or the information contained therein.

When an unauthorised user penetrates or circumvents cybersecurity measures to gain access to a system's protected areas, this is referred to as a security breach. A human, such as a cyber hacker, or a self-directing programme, such as a virus or other type of malware, could be the perpetrator.

Security lapses can occur as a result of either intentional or unintentional behaviour. In most cases, an intentional security breach is 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 personal or political gain (as in cryptojacking attacks), or to crash the network itself. As frightening as these attacks can be, they are frequently easier to detect and plan for than unintentional breaches caused by a combination of error and negligence.

Types of data breaches

A security breach and a data breach are not synonymous, despite the fact that the terms are frequently used interchangeably. A security breach is a breach of cybersecurity controls, but it does not always imply that sensitive or private data has been compromised. A "data breach" occurs when secure information is accessed by an unauthorised user or released into an untrusted environment.

There are seven distinct groups:

1. **Intrusions by hackers**

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

2. **Insider Danger**

Insider threat is a particularly dangerous type of data breach in which an employee (or vendor) gains access to and compromises data, usually for financial gain.

3. **Data in Motion**

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 become lost or damaged during the process.

4. **Theft of Physical Property**

While most businesses protect their IT networks with firewalls and cybersecurity software, they must also contend with the possibility of someone walking out the front door with a company laptop containing proprietary and potentially sensitive information.

Social engineering techniques could also be used by thieves to gain access to a secure location and download data onto a portable drive.

5. **Errors made by Humans**

Unfortunately, errors do occur. They are quite common in cybersecurity and data handling.

6. **Unintentional Internet Access**

Most businesses understand that exposing data to the public internet significantly increases the risk of exposure and unauthorised access. When data was primarily stored on-premises servers and accessed via LAN connections, this was less of an issue, 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, the risk of accidental data leakage or "man in the middle" cyberattacks increases.

7. **Unauthorized Entry**

Weak access controls, such as poorly monitored admin privileges or a lack of user segmentation, can result in people handling and sharing data with which they have no business. Organizations that do not have good access policies in place increase the likelihood of other types of security breaches occurring, eventually leading to costly data breaches.

What Are the Weaknesses?

Cybersecurity is, in many ways, an arms race between attackers and defenders. Attackers are constantly probing for flaws in ICT systems, which 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 malicious software or hardware to be inserted during the acquisition process; and previously unknown, or zero-day, vulnerabilities with no established fix. Even when solutions to vulnerabilities are known, they are often not implemented due to budgetary or operational constraints.

What are the Impacts?

A successful attack can jeopardise an ICT system's confidentiality, integrity, and availability, as well as the information it handles. Industrial control system attacks can destroy or disrupt the equipment they control, such as generators, pumps, and centrifuges.

Most cyberattacks have minor ramifications, but a successful attack on some components of critical infrastructure (CI), the majority of which is held by the private sector, could have serious implications for national security, the economy, and

individual citizens' livelihoods and safety. As a result, a rare successful high-impact attack can be more dangerous than a common successful low-impact attack.

Typically, managing cyberattack risks 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 vary depending on the industry and organisation. Customers may expect a lower level of cybersecurity from an entertainment company than they would from a bank, hospital, or government agency.

Preparing for a Security Breach

Preparation is essential when it comes to recovering from a security breach. Without the proper tools, you may not even be able to detect, let alone contain and eliminate, a security breach.

Here are some important steps to take to protect your organisation from a security incident. The better prepared you are for an attack, the faster you will be able to respond. As a result, the consequences of a cybersecurity breach are mitigated.

Recognizing your IT Assets

If you want to account for all of the resources you need to protect—and possibly replicate—as part of your recovery plan, you must conduct a thorough audit of your network's IT assets.

Add an Intrusion Detection System

The ability to detect a breach is critical for ensuring a timely response that minimises damage while also facilitating recovery and risk mitigation. Intrusion detection systems (IDSs) help you detect security breaches and respond to them as quickly as possible. Intrusion prevention systems (IPSs) go a step further by initiating network breach response measures that aid in the immediate containment of the attack. SIEM (security information and event management) systems can assist in gathering information about a network hacking attempt in order to reveal the attack methodology, which can be used to prevent future attacks.

Create an Incident Response Plan

An incident response plan (IRP) is a document that specifies what each employee in the organization should do in the event of a network breach. With an IRP in place, employees can respond to network hacks more quickly and consistently, allowing the breach to be contained and eliminated faster. Setting up an incident response plan entails distributing the plan to all employees in the organization and ensuring that they understand and can meet the IRP document's expectations. Additional

training sessions or meetings may be required to go over the plan's contents and explain how to use specific tools required to detect, contain, and eliminate a network breach.

Backup Your Data

It is critical to create a remote data backup of your organization's most critical information prior to an attack so that local files can be restored in the event of a network breach. This helps to prevent data loss due to breaches that damage or encrypt locally stored files. It is also an important part of a disaster recovery (DR) plan. Naturally, establishing the backup necessitates categorizing all of the organization's data in order to preserve the most critical information in the event of an emergency. Trying to copy everything causes 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).

Conduct Routine Penetration Testing

Penetration tests are an important risk mitigation tool because they detect flaws in your security preparations and allow you to address them before a breach occurs. A penetration test (also known as a "pen test") is a deliberate attempt to breach your cybersecurity architecture by cybersecurity experts. This aids in the identification of potential network exploits, which you can then fix to prevent attackers from exploiting them in a "zero day" attack. These tests should be carried out on a regular basis, particularly following major changes to your organization's software or IT hardware.

Create an Incident Response Team (IRT)

While having an incident response plan is beneficial, it is equally important to have the right people with the right skills and experience to handle your response to a security breach. An incident response team, whether comprised of internal IT personnel or a third-party cybersecurity staffing provider, can assist in ensuring that your IRP runs as smoothly as possible. Your IRT personnel will collect, analyse, and act on information about security incidents. Some organisations refer to this as a computer security incident response team because they may have to deal with incidents other than data or network breaches (CSIRT).

How to respond to a Security Breach

When a security breach occurs, businesses must have a clear plan of action in place. The incident response plan should be the guiding light in these situations. The plan should have been widely distributed throughout the organization to ensure that everyone is aware of their roles and responsibilities in the event of a cybersecurity incident.

Phase One of Breach Recovery: Attack Prevention

Recognizing that there was a breach was the first step toward recovery. The sooner a breach is detected, the better off your company will be.

The second step is to contain the breach, which entails preventing the attacker from gaining access by isolating the compromised system(s) or revoking the user account's access privileges.

After the threat has been contained, the third step is to eliminate it. The method of elimination may differ depending on the type of breach. To completely remove a ransomware threat, for example, all affected data storage media may need to be formatted (or even physically removed and replaced). Data that has been destroyed can then be recovered from a remote backup (assuming one exists). You can mitigate the damage caused by a breach if you can identify, contain, and eliminate it before the attacker gains access to the compromised system.

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

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

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

Save activity logs from the time of the breach for later forensic analysis. These logs can help you determine the source of the attack and prevent similar attacks in the future.

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

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

In general, the earlier you can send a notification, the better. Contact methods for notification may differ, and it is often a good idea to send notifications through multiple channels whenever possible to ensure that those affected by a breach are notified. You could, for example, notify customers via mass email, regular mail, or automated phone calls that they may have been affected. Include the date of the breach, what types of files may have been compromised, and what precautions the message recipient should take based on the type of data compromised in the email/mail/phone message. Following a breach, sending these types of notices is critical for preserving your company's reputation.

Phase Four of Breach Recovery: Restoring Network Assets

Individual network assets that have been compromised can be restored in a variety of ways, depending on how you prepared for the security breach. In some cases, simply wiping or replacing the affected IT assets' data storage drives and downloading any lost data from a backup may be sufficient. In other cases, you may be able to activate complete cloud-based replicas of your network environment in order to quickly restore your company's network. Essentially, your business continuity (BC)

and disaster recovery (DR) plans will dictate how you restore assets on your network. A BC/DR plan should be created well in advance to create fail-safes so that if one of your assets fails, your business can continue to operate.

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 when restoring assets.

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

Following your BC/DR plan to recover from the attack, it is critical to prepare for the next attack. If you've already been hit, you're likely to be attacked again by the same group—or by others using the same attack strategy.

You can identify and close the gaps in your cybersecurity that allowed the attack to occur by investigating the attack method and determining how the attacker(s) gained access. Regular testing would also be a viable option for preventing attacks. This can aid in the prevention of future breaches. Furthermore, researching the implementation of your BC/DR plan can teach you how to improve the plan in the future. Making these changes can help you respond to an attack faster and reduce downtime and disruption caused by an attack.

Legislative Actions and Proposals

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

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

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 cybersecurity 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 cybersecurity workforces.

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.

References

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

Cybersecurity Issues and Challenges: In Brief Eric A. Fischer

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 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.

7 Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," October 2011, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf