Unit 10 Planning for Privacy Breach

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Understand the importance of preparing in advance for a privacy breach
- ✓ Discuss the steps to be taken when planning for privacy breach incidents
- ✓ Identify the primary goals of an effective privacy breach prevention policy

Unit 10

Planning for Privacy Breach

Privacy Issues Must Be Prioritised By All Organisations

On a growing basis, countries around the world are recognising privacy as an essential human right. Particularly in an era of near-total connectivity on a global basis, authorities worldwide are acknowledging the importance of privacy and the protection of private data. Fundamental privacy principles have been around for some time, but it is only as of late that serious privacy breaches and related issues have become daily occurrences. The bigger the threat posed to the privacy of any given individual or organisation, the more important it is to ensure they are sufficiently protected.

Increasingly, the general public is demonstrating a good degree of awareness and competence when it comes to privacy issues. As a result, businesses of all sizes spanning all sectors cannot expect to get away with substandard security policies. Today, every organisation must do everything within its power to safeguard its customers and their privacy, in order to maintain their trust, respect and loyalty. Where incidents involving customer data occur, it can have a catastrophic impact on the reputation and performance of the entire organisation.

Businesses in general are gradually upping their game where privacy matters are concerned, but evidence suggests there is still a long way to go. In addition, it is unlikely a point in time will ever be reached where *all* potential attacks and breaches can be eliminated from the equation. As a result, businesses of all sizes must ensure they are sufficiently prepared for a privacy breach, which could occur at any time.

A Dynamic Range of Threats and Exposures

All businesses must contend with an extensive range of threats that can manifest in a variety of ways. Stolen computer systems and attacks carried out by hackers are the most common threats, but businesses must also contend with issues such as human error, accidental damage, lack of awareness on the part of those handling personally identifiable information, deliberate attacks carried out internally (by members of the workforce) and so on.

In any case, the one thing that can be said across the board is that data protection issues and privacy breaches are becoming more commonplace than ever before. Not only are the attacks mounted by perpetrators becoming increasingly sophisticated, but the fact that we are so reliant on connected technology leaves each and every one of us wide open to attack. Every time you submit or even save personally identifiable information on a connected digital device, there's a chance it could be accessed and used by anyone wishing to do so.

What's important to remember with privacy incidents is that the potential consequences extend far beyond the immediate costs. Particularly in the case of businesses who fall victim to such attacks, the damage

caused to an organisation's reputation and trust could be catastrophic. Perhaps irreparable, in the worst instances.

Hence, the number one rule when it comes to data protection and privacy is also the simplest:

Prevention of a privacy breach is better than response and recovery.

Where an organisation of any kind utilises the private information of clients, customers, suppliers, financial partners or anyone else at all, they are a potential target for criminals. Quite simply, there isn't a single business worldwide that is immune to these kinds of attacks.

This is why businesses across the board need to ensure that they have the knowledge, resources and response mechanisms in place to deal with any incident that may occur. The development and implementation of robust data protection policies is essential, as is creating and testing an effective breach response plan.

Much of the world is moving towards a point where multi-dimensional protection of privacy when handling the PII of others is a legal requirement for the business. Particularly in regions like the European Union, the United Kingdom and United States, businesses are facing increasingly heavy scrutiny with regard to their data protection policies.

If a breach occurs and the organisation is found to have been flouting its responsibilities, the consequences could be devastating.

Steps to be Taken when Planning for a Privacy Breach

There are five primary steps to be taken when planning for a privacy breach, as outlined below:

1. Identify and define the possible privacy breaches
2. Create plans for dealing with these breaches
3. Ensure you know exactly when a breach occurs
4. Know when to provide notification for those affected
5. Implement immediate and ongoing recovery activities

We'll now take a look at each of these five steps in a little more detail.

Define Possible Privacy Breaches

It is only possible to plan for a potential privacy breach and address it effectively after identifying and defining it. Businesses may be targeted in a variety of different ways, just as attacks can be mounted by any number of different perpetrators.

Just a few examples of some of the most common privacy breach types encountered by organisations on a regular basis include the following:

- Unauthorised access to networks and IT systems
- Stolen or lost computer hardware and peripherals
- Unauthorised use of computers and laptops
- Unauthorised access to business premises
- Authorised users dishonestly using PII
- Hackers gaining access to private information
- Fraudulent activities, carried out internally or externally
- Hard copies of information (paperwork) falling into the wrong hands
- Accidental distribution of PII to the wrong recipients
- Compromised passwords or access credentials
- Attacks mounted by disgruntled employees or customers
- Attacks carried out by dishonest competitors

Only by understanding the various different types of privacy breaches does it become possible to plan for, identify and prevent such incidents accordingly.

Create Your Privacy Breach Response Plans

Creating plans for dealing with these kinds of breaches follows next, which begins with carefully considering the types of PII your organisation utilises. This means taking stock of *all* PII your organization collects, stores, uses and distributes, along with where it is located, who has access to it and so on.

As for what defines PII, there is no universally agreed definition for the term. Nevertheless, any information that could be used to identify a specific individual (alone or when used in conjunction with other information) is regarded as PII. Hence, pretty much *all* information collected from anyone for any purpose should be considered PII and handled with the utmost care.

Knowing what types of PII your business collects and uses is important, but so too is knowing where it is located. This is why locating and documenting the presence of PII at all levels throughout the business is essential for creating a privacy breach response plan.

Every hour of every day, businesses collect, store and utilise a staggering quantity of potentially sensitive information. Some of which is transferred textually by way of emails and written documents, other

information is communicated by telephone, some is sent directly as digital files and so on. Even with a relatively small organisation, the amount of PII on hand at any time could be enormous.

Here are just a few of the things you should be doing at this stage in the process:

1. Ensure you are up to speed with all applicable laws and regulations
2. Carefully assess what is considered PII in your jurisdiction
3. Create a detailed inventory of all the PII your organisation uses
4. Document all the different types of PII you collect and use
5. Assess and record where and how PII is collected
6. Assess and record where and how PII is stored
7. Identify and record where and how PII is transmitted externally
8. Consider who has access to the PII your organisation collects

Essentially, you are looking to create a detailed snapshot of your PII collection and usage practices, ensuring you know exactly how much PII you are dealing with, how it is collected and where it is stored.

Create the Breach Response Plan

Once you have established the different kinds of privacy breaches that can occur and your PII handling and storage practices, you can begin the process of creating an effective response plan. The idea being that with the information you have collected so far, you're able to establish safeguards to prevent incidents from occurring and deal effectively with any attacks or incidents that slip through the net.

Every incident response plan will be unique to the organisation that devises it, though in all instances will feature similar essential components.

Detailed below are 20 of most important components (almost) every privacy breach response plan should include:

1. Ensure the potential privacy breach is identified and the required notification is issued (automated or manual notification).
2. Establish the type of incident that took place, the location, the individuals involved, which systems and components have been affected, if PII is involved in the incident and so on.
3. Ensure the incident response team is notified and provided with the necessary information.
4. Establish whether the breach has concluded or is ongoing - i.e. whether that attacker is still conducting the attack at the time, in which case the systems affected may need to be shut down.

5. Determine whether or not your organisation is the primary owner of the data (it was collected directly from clients or customers) or was obtained from a third-party you do business with.

6. If you are not the primary owner of the data, ensure the owner is informed immediately.

7. Carefully consider your obligations with regard to the data you sourced from the third-party and make sure these obligations are fulfilled.

8. Work with the owner of the data to determine the potential severity of the attack and the anticipated consequences.

9. Decide whether or not it will be necessary to report the matter to the appropriate authorities, along with which authorities need to be contacted and when.

10. If you are the primary owner of the data, analysis will need to be carried out to determine which types of data are involved and how the individuals concerned (who the data relates to) may be affected.

11. Determine the jurisdictions within which all impacted individuals reside.

12. Identify the notification requirements for each of the jurisdictions.

13. It may not be a legal requirement to notify those whose PII may have been accessed, stolen or misused, but it is nonetheless considered good practice and important to do so.

14. Consider the extent to which your business will need to support the individuals impacted by the attack, which may include things like reimbursement of loss monies, telephone consultations and so on.

15. Determine the best way to notify those who may have been affected by the attack, which could be via email, direct telephone calls or a broad notice of a potential data breach on your website or social media page.

16. Send the notifications at the right time.

17. Prepare for questions and queries submitted by local and national media outlets, which may wish to cover the story and publicise the incident.

18. Carefully consider how and why the attackers were able to carry out the attack in the first place, making the necessary updates to policies and procedures to prevent similar incidents from occurring in the future.

19. Consult with outside authorities, agencies and service providers if necessary, to ensure your improved safeguards are sufficiently robust.

20. Continuously monitor the impact of the breach and provide the information, answers and support those affected need to address the issues they may have faced.

This is merely a brief summary of just a few of the key stages of a privacy breach response plan. Though again, all privacy breach response plans are unique to the organisations devising and implementing them.

When creating, implementing and improving a privacy breach response plan, it is important to be mindful of the main objectives of this type of incident handling:

- To bring the situation under control as quickly as possible
- To minimise any potential damage caused by the incident
- To ensure as much evidence as possible is preserved
- To make sure those affected by the breach are notified accordingly
- To facilitate a fast and complete recovery from the incident
- To monitor the ongoing impact and effects of the breach
- To learn from mistakes and prevent future occurrences

When you have devised what you believe to be an effective response plan, it should be clearly communicated throughout all levels of your organisation. In addition, anyone who will be involved directly in the breach response should be provided with the appropriate training and education where required.

All incident response plants should be tested at least once a year and updated regularly, in order to remain both effective and relevant.

Know When a Privacy Breach Has Occurred

Knowing when a privacy breach has occurred isn't always easy, as most data security issues occur silently and invisibly. There are various sources that may bring a privacy breach to your attention, including but not limited to the following:

- Customers
- Automated alerts
- Employees
- News outlets
- The general public
- Business partners
- Associated businesses

- Suppliers and vendors

In addition, reports of potential privacy breaches may be directed at several different departments - HR, customer service, technical support and so on. As a result, it is essential for those staffing such departments to know when and where to spot the signs of a potential breach, which can be surprisingly subtle during the early stages.

Generating awareness of the importance of identifying and reporting potential privacy breaches on a company-wide basis is essential. Even with the most advanced automated safeguards in place, it may be down to the personnel of your business to identify and report unusual activity.

At which point, those concerned must know how to report it, who to report it to and the extent to which they will play a role in the subsequent response activities.

Breach Notification

In most jurisdictions, it is now a legal requirement to notify those affected when a privacy breach occurs and PII is involved. Examples of parties that may need to be notified include the following among others:

- Clients and customers
- Business partners
- Vendors and suppliers
- Financial service providers
- Local and national news media
- Internet service providers
- Telecommunications providers
- Solicitors and legal advisers
- Regulatory agencies
- Local government offices

In short, it is a fundamental requirement to ensure that those who may be affected by the privacy breach are made aware of the incident, along with the potential consequences of the attack.

Notification may not be necessary, if there is no suspected or confirmed access to or compromise of PII. However, if there is even the slightest risk of PII being compromised by the attack, the business is formally obliged to let those affected know.

There are various methods by which those affected by a data breach can be notified, including but not

limited to the following:

- **Written communications** - sent directly via post (ideally recorded or registered) and providing detailed information about the incident and its potential consequences.
- **Telephone communications -** if you have the manpower and resources needed to call each affected party personally, it can be a great way of explaining what has happened and giving them time to relay their questions and concerns.
- **E-mail communications -** most organisations choose not to report data breaches by way of e-mail, due to the fact that such messages may be filtered and never received. It's also possible that the e-mail will simply be ignored and written off as spam.
- **Website or social media notice -** useful if you have an extensive number of individuals and entities to contact, though this typically should not be the *only* form of communication you use.
- **Notification via the media** - another form of supplementary communication, which should be used alongside a primary communication method, such as a written or telephone notification.

There are some guides to privacy breach detection and prevention that suggest those affected should be notified no later than 45 days after the date of the breach. In reality - at least by modern standards - this would be considered an unacceptable delay.

Ideally, you should be looking to notify those affected as quickly as possible after the incident takes place. Given that their personally identifiable information may have been accessed and may subsequently be used without their authorisation, they need to be made aware of the situation immediately.

The longer you wait, the more likely it is those affected will suffer adverse consequences and hold *you* responsible.

Recovery Activities

Getting things back on track in the wake of a privacy breach can be difficult, costly and time consuming. In the event that any kind of system or network compromise enabled the attack to take place, steps will need to be taken to ensure ongoing and/or repeated access is prevented.

Examples of which include the following:

- Install appropriate security patches and fixes
- Remove and reinstall software that may have been compromised
- Immediately change all login credentials and account passwords
- Restore data from trusted backups

- Enhance all physical and virtual safeguards (firewalls etc.)

The field of privacy breach prevention and data protection is one of a certain amount of trial and error. Learning from mistakes and building on past experiences holds the key to enhanced privacy and data protection, though it is (of course) better to prevent such mistakes from occurring in the first place.

Even when an incident has been identified and fully resolved, there's still much that needs to be done to ensure a robust response and to safeguard your business from future attacks.

This includes:

- Assessing and documenting the time and resources used to address the issue and the level of damages incurred.
- Conducting a detailed investigation as to the cause of the incident, in order to enable effective safeguards to be put in place.
- Communicating with clients, customers, business partners and personnel to allay concerns and continue rebuilding trust.
- Modifying your incidence response plan based on its effectiveness (or otherwise) when tending to the most recent issue.
- Providing adequate training and educational opportunities for all personnel who handle or work with PII of any kind.
- Ensuring those who were affected by the breach are made aware of the efforts being made to prevent future breaches from occurring.
- Working with local and national news media to rebuild your reputation through positive PR and by showing your effective ownership and handling of the incident.

Further Reading: