Related content

What you need to know about mandatory reporting of breaches of security safeguards

Report a privacy breach at your business

Preventing and responding to a privacy breach

September 2018

The information below provides businesses with some best practices for preventing a privacy breach and what do if a breach happens.

Understand the threats you're facing

1. **Know what personal information you have, where it is, and what you are doing with it.** Data inventories and process maps will help ensure you know exactly what personal information you need to protect, as well as when and where you need to protect it. When and where do you collect personal information? Where does that information go? Who can access it, and what do they do with it? You must understand your data before you can protect it!
2. **Know your vulnerabilities.** Conduct risk and vulnerability assessments and/or penetration tests within your organization to ensure that threats to privacy are identified. Don't just focus on technical vulnerabilities, though. Are third parties collecting personal information on your behalf without appropriate safeguards? Do you use paper-based application forms, which are transferred to a central location (the loss of which means you'll have no way of knowing who the affected individuals are, let alone how to notify them)? When you upgrade your systems, do the old systems and databases remain active, unwatched and unpatched? The OPC has seen each of these scenarios lead to a breach. Identify your organizations' weak points before a breach identifies them for you!
3. **Know your industry.** Be aware of breaches in your industry. Attackers will often re-use the same attacks against multiple organizations. Pay attention to alerts and other information from your industry association, or whatever your source of industry news – don't be the next vulnerable target!

Think beyond the hacker

4. **Encrypt laptops, USB keys and other portable media.** Organizations often focus on privacy breaches caused by hackers, but this ignores some key threats. Perhaps the most common type of preventable breach seen by the OPC occurs due to loss or theft of unencrypted laptops, USB keys, and other portable media. In many of these incidents, the use of sufficiently strong encryption could have turned a headline-grabbing privacy breach into a minor issue!
5. **Limit the personal information you collect, as well as what you retain.** You should know not only why you are collecting each piece of personal information, but why you are keeping it. Where possible, don't collect personal information. For example, in most identity authentication cases it is enough to view, but not record, an individual's identification. Also, if personal information is only collected for limited purposes, securely dispose of it after they have been fulfilled. Always keep in mind: you can't lose what you don't have!
6. **Don't neglect personal information's end-of-life.** It is important that you protect personal information throughout its lifecycle – including the often overlooked end-of-life. Clearly define your policies and procedures about the secure destruction of personal information, and make sure they are followed. The OPC has seen breaches caused by documents left behind in a move or thrown in the garbage, as well as by information not being properly erased from discarded or recycled electronics. Like an action movie hero, personal information tends to survive and reappear when its destruction isn't seen through to the end!
7. **Train your employees.** Policies can only be effective when those responsible for implementing and abiding by them are aware of what they contain, why they exist, and the consequences of neglecting their responsibilities. You should have in place ongoing privacy and security training and awareness programs that go far beyond 'box-ticking' exercises. Employees who fully understand their roles and responsibilities in protecting personal information can be one of an organization's best lines of defense against privacy breaches!
8. **Limit, and monitor, access to personal information.** Employees' access to personal information should be limited to what they need to know, particularly when this information is sensitive. This can help ensure they don't become the cause of a breach, either accidentally or intentionally. Similarly, monitored access logs can help you identify unusual behaviours, and potentially prevent an incident either before it occurs or in the early stage. Don't burden your employees with more information than they need to do their jobs!

But don't forget about hackers, either

9. **Maintain up-to-date software and safeguards.** This is Security 101: if you don't protect yourself against known vulnerabilities, you greatly increase the likelihood of a breach. Establish systematic, documented processes to ensure security-related patches are applied in a timely manner, and that software that is no longer in use is removed from your system. As well, ensure that the virus and malware definitions associated with your anti-virus and anti-malware software are current by allowing them to perform regular updates. Operate at the speed of your attackers!
10. **Implement and monitor, intrusion prevention and detection systems.** An organization's first goal is to prevent intrusions, and you should have systems in place to do so. However, the reality is that even with the best protections in place, your system may get breached. Measures such as intrusion detection systems, firewalls and audit logs can help you to identify and respond to privacy breaches before they escalate – assuming you're paying attention to them. Ensure that safeguards used to monitor network or system activities and mitigate threats have been properly implemented and are proactively monitored. Don't rely only on the guards you've posted at your gate; know what's happening inside your walls!

Breach containment and preliminary assessment

11. **You should take immediate common sense steps to limit the breach.**
    - Immediately contain the breach (e.g., stop the unauthorized practice, recover the records, shut down the system that was breached, revoke or change computer access codes or correct weaknesses in physical or electronic security).
    - Designate an appropriate individual to lead the initial investigation. This individual should have appropriate scope within the organization to conduct the initial investigation and make initial recommendations. If necessary, a more detailed investigation may subsequently be required.
    - Determine the need to assemble a team which could include representatives from appropriate parts of the business.
    - Determine who needs to be made aware of the incident internally, and potentially externally, at this preliminary stage. Escalate internally as appropriate, including informing the person within your organization responsible for privacy compliance.
    - Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action.
12. **Prevention of future breaches:** Once the immediate steps are taken to mitigate the risks associated with the breach, organizations need to take the time to investigate the cause of the breach and consider whether to develop a prevention plan. The level of effort should reflect the significance of the breach and whether it was a systemic breach or an isolated instance. This plan may include the following:
    i. a security audit of both physical and technical security;
    ii. a review of policies and procedures and any changes to reflect the lessons learned from the investigation and regularly after that (e.g., security policies, record retention and collection policies, etc.); and
    iii. a review of employee training practices; and iv) a review of service delivery partners (e.g., dealers, retailers, etc.).

▶ Report a problem or mistake on this page

▶ Was this page helpful?

Date modified: 2018-09-17