Diocese of Dunedin

Cyber Security Guidance

Contents

1. Background

The continued growth in technology and internet use in recent years has seen a significant rise in those looking to exploit unsuspecting victims for financial gain or to cause damage and interruption to systems and services. Churches, being largely staffed by volunteers, are particularly vulnerable, and both employees and volunteers can cause significant damage to the Church either deliberately or by accident through poor cyber security.

Many cyber-attacks use indiscriminate approaches to target victims, and the attackers may not be aware, and certainly don't care, that they are targeting a church or charity.

In many cases, attackers will simply see churches as an 'easy mark' and exploit the fact that we have a desire to help people (and can therefore be viewed as gullible!).

A cyber security breach can involve disruption and data loss, damage through loss of intellectual property, denial of access to websites and services, physical loss or damage through viruses, ransomware and other forms of malicious software.

We may also be open to prosecution if as churches we are inadvertently responsible for the release of personal information belonging to other people as a result of poor cyber-security.

This Photo by Unknown Author is licensed under CC BY-SA-NC

2. Cyber threats

2.1 Loss of data and Privacy Breaches

The Privacy Act 2020 defines a privacy breach as occurring when an organisation or individual either intentionally or accidentally:

- Provides unauthorised or accidental access to someone's personal information.
- Discloses, alters, loses or destroys someone's personal information

A privacy breach also occurs when someone is unable to access their personal information due to, for example, their account being hacked.

Under the Privacy Act 2020, if your organisation has a privacy breach that either has caused or is likely to cause anyone serious harm, you must notify the Privacy Commissioner and any affected people as soon as you are practically able.

The Office of the Privacy Commissioner expect that a breach notification should be made to their Office **no later than 72 hours** after you are aware of a notifiable privacy breach.

At the same time, if the person or organisation to which the data relates suffered a financial loss, or harm to their reputation because of your failure to adhere to these responsibilities, a civil liability could be created.

Other material costs could include:

- a complainant's legal costs (in the event you were unsuccessful in defending a legal action),
- your own legal defence costs.

The costs to a church following an unauthorised or inadvertent loss of data are not limited solely to legal costs and any amounts of compensation you may have to pay.

You may also incur costs:

- investigating the extent of the issue, which may include hiring professional help.
- informing affected parties that their data has been lost or illegally accessed.
- providing support to affected parties, which may include providing specialist help because of the effects of identity theft.
- reducing the impact of a loss of data on your reputation, which may include legal and publicity costs.

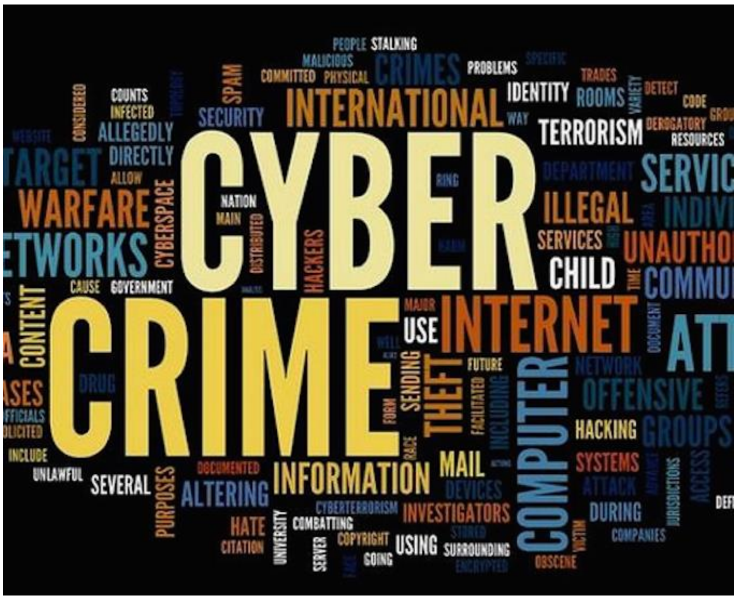
In addition to any legal liability that may be incurred by a data loss, a church could also find themselves liable for damage to third parties through unintentional onward transmission of Malware, or through their computer system being maliciously taken over and involved in a Distributed Denial of Service attack (DDoS) on other organisations.

2.2 Cyber crime

You are more likely to be affected by cyber crime than physical robbery or theft. Cyber criminals operate in organised gangs and continually find new and more sophisticated techniques to access data and information for financial gain and to commit fraud. This can result in money being taken from a bank account or credit arrangements (such as loans or overdrafts) being arranged in your organisation's name for the benefit of a fraudster. There is also an increasing risk of the use of 'Ransomware' where an attempt is made to extort money from you by preventing access to your computer system or files until a ransom is paid.

In the event that someone attempts to extort money from you, or hold your data or systems to ransom it's important that you do not pay the ransom demand without first seeking specialist advice. Paying even a small sum can result in an increased risk of you being targeted again in the future, as criminals share this information and in many cases, despite payment, access to the locked computer or files is not always restored.

Hackers will use any means available to find technical or physical vulnerabilities which they can exploit. They will use information such as LinkedIn and Facebook, and other social media to exploit people's naivety and goodwill to find further, less openly available information, which they can then use to access to your computer systems.



This Photo by Unknown Author is licensed under CC BY-SA-NC

Criminals will use a variety of methods to fool you into disclosing information:

2.2.1 Phishing

sending fraudulent emails which pretend to be from reputable organisations/authorities to trick you into revealing personal information, such as passwords and financial information.

2.2.2 Spear phishing

sending emails which appear to be from a known or trusted sender to persuade targeted individuals to reveal confidential information.

2.2.3 Whaling

sending emails which appear to be from a known or trusted sender to senior people in the organisation to get them to reveal sensitive information such as employee, volunteer or parishioner data, passwords, and other account details.

2.2.4 Smishing

sending text messages supposedly from reputable organisations/authorities which encourage people to reveal personal information, such as passwords and financial information, often by following a 'link' in the text message.

2.2.5 Vishing

Using phone calls or voicemail pretending to be from reputable organisations/authorities to trick you into revealing personal information, such as passwords and financial information.

2.2.6 Baiting

Claiming to have ‘found’ a USB drive which someone has lost, or leaving a USB stick around in a public place to be found, which when inserted into computers or network devices will deploy a payload of Viruses or Malware designed to either destroy or infiltrate the device.

2.3 Damage to computer systems

Your systems may be damaged, have access denied or even be destroyed by the use of malicious software, known as Malware, that can spread throughout a network. Systems may also be damaged through hacking (breaking security access codes to gain entry to your system). This may be through criminal action for financial gain, hacktivism (hacking for political or other cause), simple malicious intent or a need to ‘show off’ to other hackers.

Types of Computer attack can include:

2.3.1 Malware

software which is specifically designed to disrupt, damage, or gain authorized access to a computer system.

2.3.2 Denial of Service (DoS/DDoS)

a flood of simultaneous requests sent to a website to view its pages, causing the web server to crash or simply become inoperable.

2.3.3 Web attacks

websites can be defaced, databases with employee or volunteer details can be extracted, malware can be inserted for download or the details of visitors to the site can be harvested.

2.3.4 Domain hijacking

a third party can gain access to your domain name if your service provider doesn’t have the right security and contact details for you, or if you don’t keep your website registration up-to-date. **This can have a disastrous impact, as your website can then be used to gather personal information for criminals, or can be replaced by a completely different website, such as a pornography or fake commerce site.**

2.4 Business interruption

Any incident of hacking, malware or ransomware attack may mean that your computer systems are out of action and could potentially leave you unable to access information or contact details. This can result in loss of income, or additional expense to minimise the impact of this interruption to your organisation (for example, temporary hire of replacement computer equipment).

There is also a risk of reputational damage following a loss of data with parishioners, volunteers or the public losing confidence in your ability to protect their personal information, and therefore being unwilling to let you hold their information (even on a parish roll or contact list!)

3. Risk management

Most potential Cyber Crime can be prevented by taking sensible security measures, and thinking twice before opening and responding to contacts. It is still important though to **get in touch with your Privacy Officer (or the Diocesan Office) as quickly as possible if you have a privacy breach – see the Diocesan Privacy Policy for more details on reporting a breach.**

3.1 Important steps to take

3.1.1 Back up your data

- Identify important data you need to back up (such as **personal contact information**, important documents to keep the church running, **financial information** etc.)
- **Back up your data**, keep your back-up drives in **separate places from your computer,** and restrict access.
- Where possible, use a **3-point back-up system**, using 3 different locations to which your data is backed up. This approach ensures that you always have access to your data even if one or more of your backup sources is compromised or corrupted.
- Consider using a **'Cloud-based' backup** via a professional company or app so that data is physically separate from your location.
- Make backing-up part of your everyday routine. **Have a day each week (or even a time each day)** when you back up all your important information.
- If you have data that is particularly sensitive, financially important, or disastrous if lost, an IT professional may also be able to set up a **RAID ('redundant array of independent disks') system** on your drives to guard against data loss.

3.1.2 Protect your church from malware

- Make sure that you have **antivirus software** installed and running.
- Make sure that your **firewall** is switched on
- Keep all your IT equipment up to date, including **software and driver updates** and patches
- Restrict the ability to download apps and software to designated individuals
- Control how USB drives (and memory cards) can be used.
- **Never open a USB stick or an external drive if you don't know from where and from whom it has come.**

3.1.3 Use the web safely

- Built in web protection with an antivirus like ESET or a plugin such as Bitdefender can stop you from opening harmful websites

- Make sure that you look for a closed padlock symbol beside the website address you are visiting, as this indicates that the site itself is secure.

3.1.4 Keep smartphones and tablets safe

- Switch on **password protection**
- Make sure lost or stolen devices can be tracked, locked or wiped
- Keep your devices and apps up to date
- Don't connect to unknown Wi-Fi hotspots.

3.1.5 Use passwords to protect your data

- Switch on **password protection**
- Use **two-factor authentication** for "important" accounts
- Set guidelines for passwords e.g. a mix of characters, numbers, upper and lower case
- **Avoid using predictable passwords**
- Change passwords regularly
- Always change 'default' passwords.

3.1.6 Avoid phishing attacks

- **Check contact details and financial information with official sources.**
  - If you receive any communication that seems to be from someone you know asking for 'help' or money, do not reply: get in touch with that person directly yourself.
  - If you are contacted by an individual, organisation, or bank, and are at all suspicious, look up the person or organisation's details and contact them via an official number or email to confirm any communications.
  - Be wary of emails from unusual addresses, and check contact details carefully before replying to new contacts.
  - Manually check that bank details for transactions are correct – contact the bank if you are in doubt.
- Restrict computer user rights to only those required for their job
- Provide training and think about how someone might try to access your information
- Make sure your staff and volunteers are aware of the obvious signs of phishing such as poor grammar and spelling, generic openings such as 'valued customer', 'urgent' requests etc.
- Ask staff and volunteers to report all suspicious emails and to ask for help if they think they might have been victims of phishing.

3.1.7 Keep your website safe

- Make sure your domain provider, website builder and internet service provider have the right details for you, and **keep these up to date**.
- **Keep your website and domain name current** – it is very helpful to have a 'roll-over' agreement in place, so that your website and domain name will be automatically renewed unless you choose to cancel and move to a new name/provider.

- If you transfer service provider, **make sure that your website and domain name are also transferred**, and that you have provided up-to-date security information to all relevant parties.
- If you run your own website, to prevent Denial of Service attacks (see 2.3.2 above), you can choose to **route all internet traffic through a DDoS mitigation system** such as Cloudflare, which can secure all your traffic for free and will offer a paid plan for extra requirements. If your website is hosted elsewhere, consult your IT provider.

4. Reporting cybercrime attacks to the authorities

It's important to report problems or attacks to the right places so that your own church and other people can be protected properly from further attacks:

- Report any online internet safety concerns and harmful digital communications issues to Netsafe: https://www.netsafe.org.nz/
- Report any cyber security issues to CERT NZ at www.cert.govt.nz or by phoning 0800 CERT NZ (0800 2378 69) Monday to Friday 7 am – 7pm.
- Netsafe and CERT NZ may in some circumstances and with your consent, share some information with Police. This is not a Police report.
- Reporting cybercrime is just like reporting any other offence. Call 111 in an emergency. For example, if you've received an electronic message with an immediate and believable threat such as "I'm coming around now and I'm going to kill you", that would be an emergency.
- For non-emergency incidents or crimes you can still report by phone using 105, online to www.police.govt.nz/105support or in person.
- To report cybercrime to Police you will need to speak with a police representative or enter it online so that the Police can get all the right information.

5. Get help, keep up to date, and find out more

Cyber threats are constantly evolving as criminals adapt to new methods and technologies, so it is important to stay up to date on cyber safety.

CERT NZ have an excellent website with information on what you need to know about cyber security issues, how to keep safe, and what to do if you have a problem:

Visit https://www.cert.govt.nz/individuals/ and https://www.cert.govt.nz/business/ to find out more. It is worth visiting these sites regularly to keep up to date with the latest and best advice.

If in doubt, ask someone you trust for help, and seek guidance from official sources before responding to any requests for your own or other people's information.

This guidance has been commended by the Diocesan Council in July 2022. Thanks to the Very Rev'd Tony Curtis and Mr Jacob Hurd-Vial for putting this resource together.