Learning Lessons from others' mistakes

An analysis of recent cyber attacks relevant to Australian non-profits.

Information compiled July 2024

9TH MIND

Organisation	Year	Attack Type	Summary	Estimated Cost	Lessons Learned
Red Cross	2022	Data Breach	The International Committee of the Red Cross suffered a cyberattack that compromised the personal data of over 515,000 'highly vulnerable' individuals.	Not publicly disclosed	Implement strong access controls, regularly update software, and ensure data encryption to protect sensitive information.
Planned Parenthood	2021	Data Breach	A data breach at Planned Parenthood exposed the personal information of over 400,000 patients.	Not publicly disclosed	Conduct regular security assessments, monitor for unusual network activity, and protect databases with strong security measures.
The Heritage Foundation	2021	Ransomware Attack	The conservative think tank suffered a ransomware attack that disrupted its operations.	Not publicly disclosed	Maintain up-to-date backups, implement network segmentation, and develop a comprehensive incident response plan.
Nonprofit Professionals Advisory Group	2021	Data Breach	A data breach exposed the personal information of clients and employees of the Nonprofit Professionals Advisory Group.	Not publicly disclosed	Secure data storage, regularly update security protocols, and educate staff on data protection practices.
Health Service Executive (HSE)	2021	Ransomware Attack	Ireland's Health Service Executive was hit by a ransomware attack that disrupted healthcare services across the country.	Over €100 million ($117 million USD) in recovery costs	Keep systems updated with the latest security patches, segment networks to limit the spread of malware, and develop an incident response plan.
AspenPointe	2020	Ransomware Attack	Colorado-based mental health services provider AspenPointe experienced a ransomware attack that exposed the personal information of 295,000 individuals.	$1.6 million in recovery and notification expenses	Regularly back up data, train staff on phishing awareness, and employ robust endpoint protection.
UNICEF	2020	Data Breach	UNICEF suffered a data breach that exposed the personal information of over 8,000 users.	Not publicly disclosed	Ensure third-party vendors adhere to strict security protocols, encrypt sensitive data, and regularly review access permissions.
Shriners Hospitals for Children	2020	Data Breach	Shriners Hospitals for Children experienced a data breach that exposed the personal information of over 60,000 patients.	Not publicly disclosed	Encrypt sensitive data, conduct regular security audits, and ensure third-party vendors adhere to strict security protocols.
Hackney Council	2020	Cyber Attack	Hackney Council in London experienced a cyberattack that disrupted its IT systems and services.	Estimated at £10 million ($13 million USD) in recovery and remediation	Implement strong access controls, regularly update security software, and conduct regular staff training.
American Cancer Society	2019	Email Scam	Fraudsters impersonated the American Cancer Society in a phishing scam targeting donors.	Not publicly disclosed	Secure email communications with DMARC, SPF, and DKIM protocols, and inform donors about potential scams.
Children's Mercy Hospital	2019	Phishing Attack	A phishing attack on Children's Mercy Hospital in Kansas City led to the exposure of 63,000 patient records.	Not publicly disclosed	Employ advanced email filtering, conduct regular staff training, and implement data loss prevention (DLP) solutions.
Boys Town	2019	Data Breach	A data breach at Boys Town, a non-profit organisation, exposed the personal information of over 100,000 individuals.	Not publicly disclosed	Implement strong access controls, regularly update security software, and conduct regular staff training.
Optus	2019	Data Breach	An Australian telecommunications company, Optus, suffered a data breach that exposed the personal information of customers, including healthcare data.	Not publicly disclosed	Encrypt sensitive data, conduct regular security audits, and ensure secure data disposal.
MaineGeneral Health	2018	Data Breach	MaineGeneral Health experienced a data breach that compromised the personal information of over 180,000 patients.	Not publicly disclosed	Conduct regular security audits, implement strong access controls, and ensure data encryption.
Save the Children Foundation	2018	Phishing Attack	Save the Children Foundation lost nearly $1 million in a phishing attack that targeted its email system.	$1 million loss	Implement multi-factor authentication, train staff on phishing awareness, and monitor financial transactions closely.
California Department of Developmental Services	2018	Data Breach	A data breach exposed the personal information of over 12,000 individuals served by the California Department of Developmental Services.	Not publicly disclosed	Protect sensitive information with strong encryption, conduct regular security assessments, and ensure secure data disposal.
NHS	2017	Ransomware Attack	The UK's National Health Service was hit by the WannaCry ransomware, disrupting services across hospitals and clinics.	¬£92 million ($120 million USD) in lost services and IT repairs	Keep systems updated with the latest security patches, segment networks to limit the spread of malware, and develop an incident response plan.
Catholic Charities of the Archdiocese of Denver	2017	Phishing Attack	A phishing attack on Catholic Charities exposed the personal information of donors and employees.	Not publicly disclosed	Implement multi-factor authentication, conduct regular phishing simulations, and educate employees on recognising phishing attempts.
American Red Cross	2017	Data Breach	The personal information of 550,000 blood donors was exposed in a data breach at the American Red Cross.	Not publicly disclosed	Secure data storage, regularly update security protocols, and educate staff on data protection practices.
YWCA	2017	Phishing Attack	A phishing attack on the YWCA exposed the personal information of donors and employees.	Not publicly disclosed	Implement multi-factor authentication, conduct regular phishing simulations, and educate employees on recognising phishing attempts.

Key Lessons for Australian-Based Non-Profits

- **Implement Strong Access Controls**: Limit access to sensitive information and ensure that only authorised personnel have access.
- **Regularly Update Software**: Keep all systems and software up to date with the latest security patches to protect against known vulnerabilities.
- **Data Encryption**: Encrypt sensitive data both at rest and in transit to protect it from unauthorised access.
- **Employee Training**: Regularly train employees on cyber security best practices, including how to recognise phishing attempts.
- **Incident Response Plan**: Develop and regularly update an incident response plan to quickly address and mitigate the impact of cyber attacks.
- **Multi-Factor Authentication**: Implement multi-factor authentication to add an extra layer of security to sensitive systems and data.
- **Regular Security Assessments**: Conduct regular security assessments and audits to identify and address potential vulnerabilities.
- **Network Segmentation**: Segment networks to limit the spread of malware and contain potential breaches.
- **Secure Data Disposal**: Ensure that sensitive data is securely disposed of when no longer needed.
- **Third-Party Security**: Ensure that third-party vendors and partners adhere to strict security protocols to protect shared data.