8 Cybersecurity Best Practices In 2018

professional advantage

2017 has been an eventful year with businesses adapting to IOT and digital transformation. Technology advances and modernisation, whilst bringing about many positive changes, has also increased risk. According to the 2017 Australian Cyber Security Centre Threat Report, cyber crime is increasing at a disturbing rate and Australian businesses continue to be a prime target. Digital extortion is not expected to slow down in the near future.

There are several cybersecurity best practices that you can adopt immediately to significantly lower your chances of being the next online fraud or ransomware victim. As the New Year begins to unfold, make these eight cybersecurity best practices part of your company's New Year's resolution.

1 Perform Proactive Risk Assessments

Some organisations assume that staying compliant with regulations is enough to protect their data. While it is a good first step, it doesn't cover all bases. Performing proactive and repetitive risk assessments will help you to better prepare for cyber threats. A typical information systems security review will identify vulnerabilities from network, server, data and applications layers. It positions you to discover and classify your assets, analyse possible threats, identify your vulnerabilities, determine risks, and analyse control mechanisms you can put in place whilst creating a control roadmap.

2 Identify Whitelist Applications

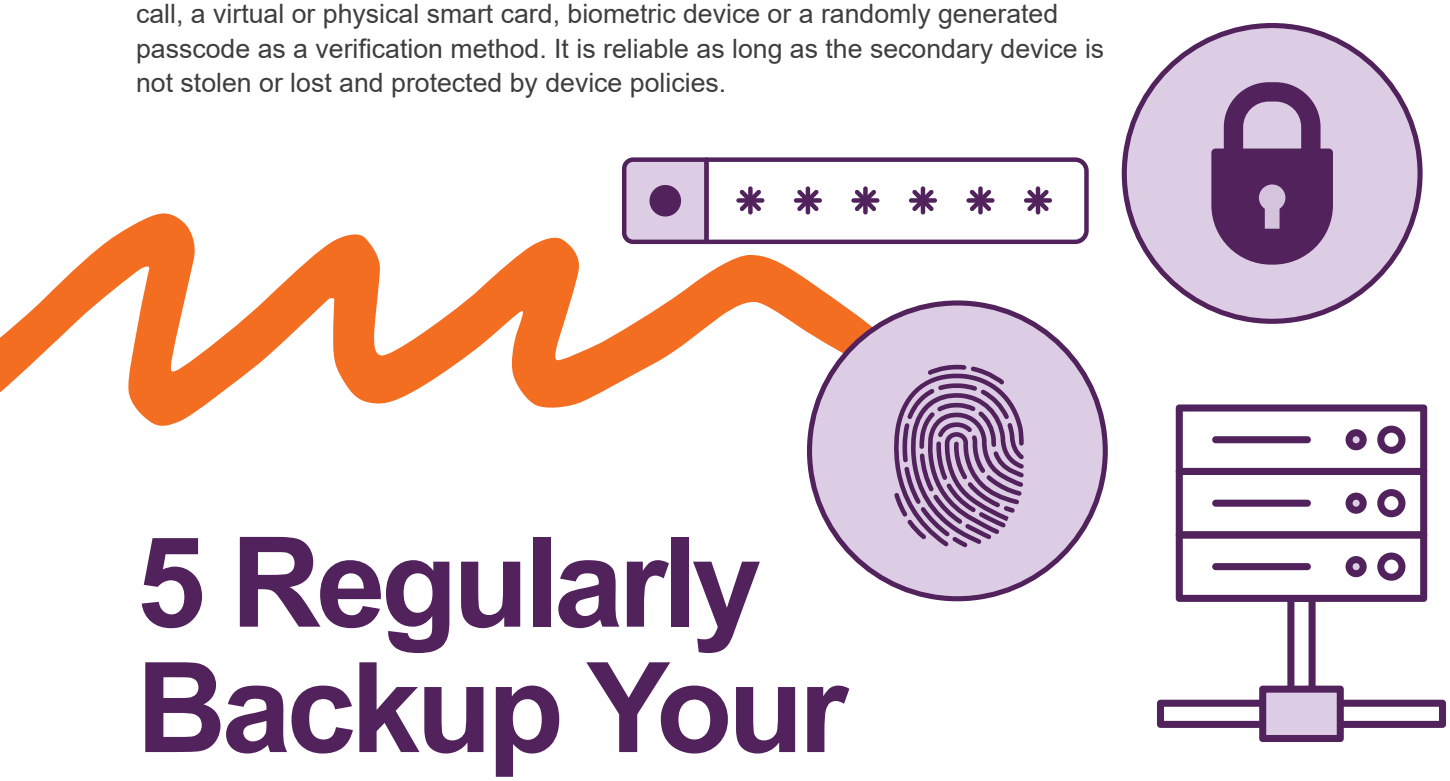
Application whitelisting is a security strategy that allows only approved applications to run on your systems blocking all other programs including malware and other malicious software. If you are using Windows 8 or 10 and Windows Server 2012 or 2016 as operating systems, you can utilise Applocker from Microsoft to create rules which allow or deny apps from running based on types of files or users.

3 Operating System and Application Patching

Leaving your Operating System (OS) or applications unpatched for updates leaves a door open for a malware attack. It is highly recommended to turn on automatic updates on your PCs and if you are using Microsoft System Center Configuration Manager (SCCM), this can be automated.

4 Use Multi-factor Authentication

Multi-factor Authentication (MFA) is one of the best ways to protect your account as it utilises an additional physical device to confirm the identity of the person accessing the account. It is an authentication method that requires either a phone call, a virtual or physical smart card, biometric device or a randomly generated passcode as a verification method. It is reliable as long as the secondary device is not stolen or lost and protected by device policies.



5 Regularly Backup Your Data

Backing up your data is critical, and should be performed on a regular basis. Back ups should ideally be stored on a protected system which will allow you to get access to it when needed. Make sure to encrypt backups for sensitive data and verify that your files are retrievable. While backing up your data doesn't stop a ransomware attack, having access to your backups will ensure the business impact isn't too severe.

6 Limit Administrative Privileges

Allowing too many people to download or use any software is dangerous! Practice limited local PC administrative privileges, especially for your new users and escalate permissions only when necessary. Restricting your users' ability to install and run applications can greatly help prevent malicious software from spreading through your network.

7 Boost Staff Awareness

Ensuring your staff are aware of cyber threats and how to recognise them is critical in fighting cyber crime. Your staff will receive numerous cyber threats through phishing scams and malware, and the next steps they take are critical in preventing further impact to the business. Explaining the impact of cyber crime will help staff adopt certain measures to protect your business and your bottomline.

8 Create an Incident Response Plan

When a security breach happens, do you know what steps to take to help detect, respond to and limit the effects of cybersecurity incidents? That is what an Incident Response Plan (IRP) is for. Being prepared ahead of time can help in limiting the damage of a breach and allow you to remediate the incident effectively. When creating an IRP, consider keeping it simple and flexible to adapt to various situations and review the plan to make sure that your documented procedures are applicable.

Let Us Help You Implement These Best Practices

Make these best practices part of your long-term strategy to protect your business from cybercrimes. However, implementing these correctly could be challenging if you don't have the depth of experience or the right skills.

Professional Advantage has a Cybersecurity Team that can help your organisation get the best protection and stay on top of the ever-evolving cyber security world.

We can help you in any of these ways:

1 Perform a network vulnerability scan and risk assessment

2 Create a back up plan

3 Implement an Incident Response Plan

For more information

1800 126 499

www.pa.com.au

enquiries@pa.com.au

About Professional Advantage

Professional Advantage is one of Australia's most awarded solutions providers, with over 25 years experience in helping organisations improve their business systems through industry leading software solutions. Our 250-strong team in 6 offices across Australia and internationally has successfully worked with over 1000 organisations.

professional advantage