cbts | Hawaiian Telcom

CYBER SAFE BASICS FOR BUSINESS

Breaches and other cybersecurity incidents cost organizations a lot of money, stress, and negative impact on their brand. It can be difficult to pick a starting point for your cybersecurity program. This guide highlights key areas that organizations can start with to get quick cybersecurity wins.

THE BASICS:

ALIGN TO A CYBERSECURITY FRAMEWORK

Cybersecurity frameworks consist of standards, guidelines and best practices to manage cybersecurity risk. They are great tools for organizations to reference on where they are and where they should be. Tools like the CIS Top 18 can help you get started.

HAVE STRONG ACCOUNT MANAGEMENT

Organizations should implement access controls like a strong password policy, multifactor authentication, and encourage the use of unique passwords through a passwords manager. Make sure you have ways of auditing and identifying if unauthorized access has occurred.

KEEP PATCHES AND APPS UPDATED

Make sure that the latest patches, operating system versions, and updates are applied to limit vulnerabilities. Patches should be automatically deployed, tested in a small group before being rolled out to the whole population, and easily reverted if a bad patch is issued. Stay informed if the community is reporting on buggy patches.

PROTECT THE ENDPOINT

Endpoint Detection and Response (EDR) is an advanced endpoint protection tool that provides greater protection through deeper system visibility. Harden your endpoints by restricting administrative rights, program installations, and scripting capabilities on your user's devices.

TRAIN THE WORKFORCE TO SPOT SUSPICIOUS ACTIVITY

Security awareness training teaches workforce how to use information systems safely and how to identify suspicious activity. Security awareness programs should be required by policy, provide training, accountability, and information on how to report suspicious activity.

LIMIT ACCESS TO SENSITIVE INFORMATION

Implement access controls to prevent unauthorized access to sensitive information that could result in a breach. Sensitive data like PII, financial, and health information should have encryption and permissions on who can access the data.

BACKUP YOUR MOST CRITICAL DATA, APPLICATIONS, AND SYSTEMS

Do regular backups of key information to ensure that the organization can recover from a cyber incident. Backups should be stored offsite, immutable, and encrypted. Cloud technologies can help organizations maintain the most uptime for their applications.

If you would like more information on how to implement these steps, please contact your Hawaiian Telcom account manager, email salessupportcorp@hawaiiantel.com or visit us at hawaiiantel.com/cbts. Follow us on our blog or join the conversation on Hawaiian Telcom University LinkedIn Group.