





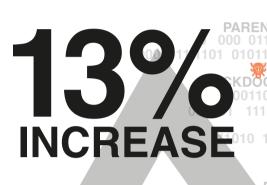
2017 HASN'T BEEN EASY

FOOD



HOSPITA

BEACHDEACH VEAR FOOD RETAIL STATE HOSPIT FINANCIAL CYBER SEC **CYBER SECURITIES**



DATA BREACHES



INCREASE

STOLEN, LOST OR COMPROMISED RECORDS



There are three primary vectors in a hospitality IT environment: User, Website and Systems.





REDUCE MISUSE BY NEGLIGENT AND/OR IGNORANT USERS

ESTABLISH A THIRD-PARTY USER EDUCATION PROGRAM TO



RESOURCES PEER-TO-PEER

SHUT DOWN THE ABILITY FOR USER TERMINALS TO SHARE



ON EXTERNAL DRIVES OR VIRTUAL MACHINES

IMPLEMENT A DATA BACK-UP STRATEGY FOR PERSONAL DATA



CONFIGURE EMAIL PROTECTION MEASURES

INSTALL A REPUTABLE ANTIVIRUS PROGRAM





AND DATABASE SERVERS

ENSURE PROPER SEGMENTATION BETWEEN WEB SERVERS



ASSETS TO PREVENT AN ATTACKER FROM GAINING FURTHER INTERNAL ACCESS SHOULD A BREACH OCCUR TRACK VULNERABILITY PATCH STATUS OF CRITICAL DATA

UTILIZE A DEMILITARIZED ZONE FOR PUBLICLY FACING



HAVE A BACK-UP STRATEGY FOR DATABASES AND FILE SHARES



MACHINES FOR CRITICAL DATA STORAGE AND FILE SHARES OFFSITE

CONSIDER USING SECURE CLOUD OR VIRTUALIZED

SERVERS AND FILE SHARES







MAINTAIN THE MOST UP-TO-DATE SOFTWARE



INSTALL A FIREWALL AND ANTIVIRUS SOFTWARE ON BUSINESS SYSTEMS



CREATE STRONG PASSWORDS FOR BUSINESS SYSTEMS AND CHANGE THEM OFTEN



MONITOR AND MANAGE ACCESS TO BUSINESS SYSTEMS AND TERMINALS, INCLUDING ELIMINATING REMOTE ACCESS