Shiji

HOTEL CYBERSECURITY CHECKLIST

BY SHIJI

It's more important than ever to protect your hotel and your guests' data. Below is our Hotel Cyber Security Checklist, by Aleksander Ludynia, Chief Security Officer at Shiji Group, which offers steps to take when developing your hotel's cybersecurity action plan. Follow these steps to ensure that you are adequately managing the risks to your customers, your property, and your reputation!

GOAL 1:

COMPLETE? YES /NO:

ASSIGN CYBERSECURITY AND PRIVACY SPECIALIST ROLES

These will be the people guiding the efforts of the rest of the personnel, as security is everyone's job.

WHO: ROLE:

- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....

GOAL 2:

COMPLETE? YES /NO:

IDENTIFY AND ASSESS RISKS FOR ALL SENSITIVE DATA

Conduct audits of all data handled by your hotel that can be considered sensitive, including systems used to process and store them. Common points are legacy systems, inexperienced or temporary staff, bad habits such as keeping passwords in unprotected places, and third-party systems. List them here.

ASSETS:

- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....

GOAL3:

COMPLETE? YES /NO:

PROTECT THE DATA AND KEY SYSTEMS

Knowing what needs to be protected ensures that you will be able to choose a security solution to apply, as well as an ideal secure configuration to harden all of your key systems. What are those key systems?

KEY SYSTEMS:

- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....
- ○ .....

COMPLETE? YES /NO:

GOAL 4:

MANAGE ACCESS AND VULNERABILITIES

Control who has access to what kind of information and for what reasons, so that each person is only able to see what is necessary for them to fulfill their duties. Cybercriminals are opportunistic, therefore vulnerability management and basic cybersecurity hygiene are key to preventing being the low-hanging fruit for these criminals.

SYSTEM:	WHO HAS ACCESS:
○	
○	
○	
○	
○	
○	
○	
○	
○	

COMPLETE? YES /NO:

GOAL 5:

MONITORING

Monitoring access regularly helps in identifying breaches or leaks early, and gives you time to react to them. Keep track of traffic of users, applications, and networks.

WHO WILL MONITOR?	FREQUENCY:
○	
○	
○	
○	
○	
○	
○	
○	
○	

COMPLETE? YES /NO:

GOAL 6:

DEPLOY MALWARE PROTECTION

Simply having an antivirus solution isn't enough. Pick the best solution, configure it properly, and make sure that it's deployed everywhere, and that it is indeed effective.

SOLUTIONS:	ROLE:
○	
○	
○	
○	
○	
○	
○	
○	
○	

COMPLETE?
YES /NO:

GOAL 7:

DEPLOY ENDPOINT PROTECTION

Endpoints (such as mobile devices, browsers, and office computers) are usually the first step in cyber attacks, and criminals use them as an access point to go deeper into the company, so ensure adequate protection.

SOLUTIONS:

ROLE:

- ○
- ○
- ○
- ○
- ○
- ○
- ○
- ○
- ○

COMPLETE?
YES /NO:

GOAL 8:

MANAGE LEGACY AND THIRD-PARTY SYSTEMS

Ensure the protection of your business data that third-party systems, such as partners or vendors, can access as they are also vulnerabilities. As for legacy systems, the lack of security patches can make them susceptible to modern forms of attack.

SYSTEM SECURITY FEATURES:

SECURE?

- ○
- ○
- ○
- ○
- ○
- ○
- ○
- ○
- ○

COMPLETE?
YES /NO:

GOAL 9:

BUILD AWARENESS AND PREPARE FOR THE WORST

Provide good training to employees on how to spot different sorts of cyber attacks. Introduce and periodically improve incident management processes with constant backups and set recovery processes in place.

TRAINING STEPS:

- ○
- ○
- ○
- ○
- ○
- ○
- ○
- ○
- ○

GOAL: 10

COMPLETE? YES /NO:

TEST YOUR SECURITY

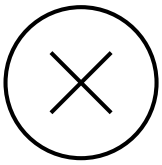
Conduct penetration testing to verify the actual security level of your systems and make sure it is up to par.

TEST NAME: ROLE:

- ○
- ○
- ○
- ○
- ○
- ○
- ○
- ○
- ○

YOUR CROWN JEWELS

- CARDHOLDER DATA
- PERSONAL DATA
- PEOPLE LOCATION
- RATES DATA
- GUESTS AND THEIR DEVICES



THREAT ACTORS

- CYBER GANGS: steal cardholder & personal data
- STATE-SPONSORED ATTACKS: target personal data and location
- COMPETITORS: steal rates