# CHECKLIST

## INFORMATION

□ How do you specify what kind of response information could be accepted?

□ Do all of your information assets need an owner?

□ Are server side checks done that solely rely on information provided by the attacker?

□ What information is important to track?

□ What information is required to reset the password?

□ Who needs to share information, and who can resolve the issues that emerge?

□ Does the application contain any business sensitive information?

□ Do you ever seek additional information about updates?

□ What type of information do you consider to be part of your intelligence gathering?

□ Is anybody already at the edge of information overload?

□ What will be the consequence of gaps in information when the initiative is rolled out?

□ What information is deemed critical and why?

□ How well protected is the information to unauthorized access?

□ How is the information actually shared securely?

□ How certain is the information included in the record?

□ What is the impetus behind information sharing?

□ Do you know where all of your information assets reside?

□ Does the solution provide a unified view of vulnerabilities, configurations, and asset information?

□ What information is being shared, and what is the purpose of sharing it?

□ Do you know what information is most valuable to the business?

□ What procedures do you have for keeping employees personal information confidential?

□ Do the logs contain sensitive information?

□ Is there a need to tailor infosec standards to certain types of information, and if so how?

# CHECKLIST

□ Is the board demonstrating due diligence, ownership, and effective management of information risk?

□ Does the cloud provider charge a fee for ediscovery/information access requests?

□ Where is the information accessed, processed, and stored?

□ What are the policies and procedures used to protect sensitive information from unauthorized access?

□ How much personally identifiable information could be disclosed?

□ Where are you suggesting putting that information?

□ Is information stored on the client that should be stored on the server?

□ Can the attacker obtain access to sensitive information as secrets, PII?

□ What are the main advantages of the current update information?

□ What information will you disclose?

□ NOTES: