



15 Minutes to a Secure Business

One hour a week—that's how much time the typical small and medium business devotes to its information system security. Use this calendar to help track what activities to do on a daily basis that ensure your business is secured in just 15 minutes a day.

	Monday	Tuesday	Wednesday	Thursday	Friday
WEEK 1	<ul style="list-style-type: none"> Identify non-compliant systems Keep non-compliant systems updated Adjust zero-day threat protection policies Monitor compliance policies 	<ul style="list-style-type: none"> Check for virus outbreaks Isolate and clean infected users Monitor compliance policies 	<ul style="list-style-type: none"> Detect rogue systems Remediate rogue systems Synchronize with ActiveDirectory Identify emerging threats 	<ul style="list-style-type: none"> Manage quarantined emails Tune mail server content filter Confirm mail server spam and AV protection Check for virus outbreaks 	<ul style="list-style-type: none"> Assess Email and Web Gateway defense Update Email and Web Gateway defense Monitor malicious web sites Review content filters at the gateway
WEEK 2	<ul style="list-style-type: none"> Check for virus outbreaks Isolate and clean infected users Assess Encryption Policy compliance Enforce disk encryption policy 	<ul style="list-style-type: none"> Identify non-compliant systems Keep non-compliant systems updated Adjust zero-day threat protection policies Enforce file & folder encryption policy 	<ul style="list-style-type: none"> Assess Email and Web Gateway defense Update Email and Web Gateway defense Monitor malicious web sites Review content filters at the gateway 	<ul style="list-style-type: none"> Detect rogue systems Remediate rogue systems Synchronize with ActiveDirectory Check for virus outbreaks 	<ul style="list-style-type: none"> Manage quarantined emails Tune mail server content filter Confirm mail server spam and AV protection Identify non-compliant systems
WEEK 3	<ul style="list-style-type: none"> Detect rogue systems Remediate rogue systems Synchronize with ActiveDirectory Identify emerging threats 	<ul style="list-style-type: none"> Manage quarantined emails Tune mail server content filter Confirm mail server spam and AV protection Check for virus outbreaks 	<ul style="list-style-type: none"> Assess Email and Web Gateway defense Update Email and Web Gateway defense Monitor malicious web sites Review content filters at the gateway 	<ul style="list-style-type: none"> Identify non-compliant systems Keep non-compliant systems updated Adjust zero-day threat protection policies Monitor compliance policies 	<ul style="list-style-type: none"> Check for virus outbreaks Isolate and clean infected users Monitor compliance policies
WEEK 4	<ul style="list-style-type: none"> Identify non-compliant systems Keep non-compliant systems updated Adjust zero-day threat protection policies Lock lost or stolen devices 	<ul style="list-style-type: none"> Check for virus outbreaks Isolate and clean infected users Assess network connected devices Adjust device control policies 	<ul style="list-style-type: none"> Detect rogue systems Remediate rogue systems Synchronize with ActiveDirectory Identify emerging threats 	<ul style="list-style-type: none"> Manage quarantined emails Tune mail server content filter Confirm mail server spam and AV protection Update network protection 	<ul style="list-style-type: none"> Assess Email and Web Gateway defense Update Email and Web Gateway defense Monitor malicious web sites Review content filters at the gateway
WEEK 5	<ul style="list-style-type: none"> Assess Email and Web Gateway defense Update Email and Web Gateway defense Monitor malicious web sites Review content filters at the gateway 	<ul style="list-style-type: none"> Identify non-compliant systems Keep non-compliant systems updated Adjust zero-day threat protection policies Check for virus outbreaks 	<ul style="list-style-type: none"> Check for virus outbreaks Isolate and clean infected users Monitor perimeter network protection Check compliance with PCI 		