Assess your security posture and understand your risks

Cybersecurity is one of the most important ongoing business concerns for any organization.

Major security risks are not limited to the Fortune 500.
On the contrary, small and mid sized businesses are often completely wiped out by the repercussions of a security breach. To address core cybersecurity risks and mitigate the likelihood of these outcomes, organizations of all industries, geographies, and sizes can begin with a risk based security assessment.

Determining where you are, and where you want to be
As part of any organization's ongoing security improvement initiatives, it's always recommended, and in many cases a requirement, to review the current (as is) state security posture and understand the need for improvement, based on the agreed future (to be) state.

Not all organizations aspire to achieve the same level of maturity; it’s driven by many factors which may include business goals, appetite for risk, security culture, budget, market vertical, regulatory compliance, and industry competition.

Benefits
• Provides organizations with the ability to understand their approach to information security
• Prioritize future cyber security investment for greatest risk reduction
• Align people, process and technology with cybersecurity and business goals

Product Brief: Cyber Risk Posture Assessment

Benefits
• Provides organizations with the ability to understand their approach to information security
• Prioritize future cyber security investment for greatest risk reduction
• Align people, process and technology with cybersecurity and business goals

Cybersecurity is one of the most important ongoing business concerns for any organization.

Major security risks are not limited to the Fortune 500.
On the contrary, small and mid sized businesses are often completely wiped out by the repercussions of a security breach. To address core cybersecurity risks and mitigate the likelihood of these outcomes, organizations of all industries, geographies, and sizes can begin with a risk based security assessment.

Determining where you are, and where you want to be
As part of any organization's ongoing security improvement initiatives, it's always recommended, and in many cases a requirement, to review the current (as is) state security posture and understand the need for improvement, based on the agreed future (to be) state.

Not all organizations aspire to achieve the same level of maturity; it’s driven by many factors which may include business goals, appetite for risk, security culture, budget, market vertical, regulatory compliance, and industry competition.
Why AT&T

AT&T has experts who can support or supplement your team when suspected unauthorized activities are detected with a full incident management program that includes: detection, triage, response, and containment and prevention planning.

To learn more about AT&T Cybersecurity Consulting, visit att.com/security-consulting