REDEFINING SECURITY PERFORMANCE AND HOW TO ACHIEVE IT

GLOBAL ORGANIZATIONS STRUGGLE TO IDENTIFY AND PROTECT CRITICAL ASSETS FROM CYBERATTACKS

WHAT IS THE ACCENTURE SECURITY INDEX?

A comprehensive benchmark measuring the alignment of a company’s cybersecurity strategy with its business imperatives, serving as a diagnostic tool to help companies understand how they stack up against their peers, industries, and countries. The index uses 33 cybersecurity capabilities, the industry and country level, helping companies understand how effective their security measures are and identifying measures to take to reduce threats.

ROOM FOR IMPROVEMENT IN 33 CRITICAL CYBERSECURITY CAPABILITIES ACROSS 15 COUNTRIES

AND 12 INDUSTRIES

SIX RECOMMENDATIONS FOR ORGANIZATIONS TO REDUCE SECURITY THREATS

1. DEFINE CYBERSECURITY SUCCESSES FOR THE ORGANIZATION
   Improve the alignment of the company’s cybersecurity strategy with its business imperatives and enhance abilities to detect and repel threats.

2. PRESSURE-TEST SECURITY CAPABILITIES
   Engage “white-hat” external hackers for attack simulations to establish a realistic assessment of internal capabilities. By pressure-testing company defenses in this way, leaders quickly understand whether they can really withstand a targeted, focused attack.

3. PROTECT FROM THE INSIDE OUT
   Prioritize the protection of key assets and focus on those internal incursions with greatest potential impact. Instead of attempting to anticipate a variety of external breach possibilities, organizations can concentrate on fewer, critical internal incursions.

4. KEEP INNOVATING
   Invest in state-of-the-art programs that help the company to outmaneuver adversaries instead of spending more on existing programs.

5. MAKE SECURITY EVERYONE’S JOB
   Prioritize training for all employees, implementing a critical role in detecting and preventing breaches and represent a company’s frontline defense, leaders must be realistic and determine which capabilities can pay disproportionate dividends.

6. LEAD FROM THE TOP
   CEOs must materially engage with executive leadership and make the case that cybersecurity is a critical priority in protecting company value.

SIX RECOMMENDATIONS FOR ORGANIZATIONS TO REDUCE SECURITY THREATS

1. DEFINE CYBERSECURITY SUCCESSES FOR THE ORGANIZATION
   Improve the alignment of the company’s cybersecurity strategy with its business imperatives and enhance abilities to detect and repel threats.

2. PRESSURE-TEST SECURITY CAPABILITIES
   Engage “white-hat” external hackers for attack simulations to establish a realistic assessment of internal capabilities. By pressure-testing company defenses in this way, leaders quickly understand whether they can really withstand a targeted, focused attack.

3. PROTECT FROM THE INSIDE OUT
   Prioritize the protection of key assets and focus on those internal incursions with greatest potential impact. Instead of attempting to anticipate a variety of external breach possibilities, organizations can concentrate on fewer, critical internal incursions.

4. KEEP INNOVATING
   Invest in state-of-the-art programs that help the company to outmaneuver adversaries instead of spending more on existing programs.

5. MAKE SECURITY EVERYONE’S JOB
   Prioritize training for all employees, implementing a critical role in detecting and preventing breaches and represent a company’s frontline defense, leaders must be realistic and determine which capabilities can pay disproportionate dividends.

6. LEAD FROM THE TOP
   CEOs must materially engage with executive leadership and make the case that cybersecurity is a critical priority in protecting company value.

SIX RECOMMENDATIONS FOR ORGANIZATIONS TO REDUCE SECURITY THREATS

1. DEFINE CYBERSECURITY SUCCESSES FOR THE ORGANIZATION
   Improve the alignment of the company’s cybersecurity strategy with its business imperatives and enhance abilities to detect and repel threats.

2. PRESSURE-TEST SECURITY CAPABILITIES
   Engage “white-hat” external hackers for attack simulations to establish a realistic assessment of internal capabilities. By pressure-testing company defenses in this way, leaders quickly understand whether they can really withstand a targeted, focused attack.

3. PROTECT FROM THE INSIDE OUT
   Prioritize the protection of key assets and focus on those internal incursions with greatest potential impact. Instead of attempting to anticipate a variety of external breach possibilities, organizations can concentrate on fewer, critical internal incursions.

4. KEEP INNOVATING
   Invest in state-of-the-art programs that help the company to outmaneuver adversaries instead of spending more on existing programs.

5. MAKE SECURITY EVERYONE’S JOB
   Prioritize training for all employees, implementing a critical role in detecting and preventing breaches and represent a company’s frontline defense, leaders must be realistic and determine which capabilities can pay disproportionate dividends.

6. LEAD FROM THE TOP
   CEOs must materially engage with executive leadership and make the case that cybersecurity is a critical priority in protecting company value.