The second annual RSA Cybersecurity Poverty Index is the result of an annual maturity self-assessment completed by 878 individuals across 24 industries. The assessment was created using the NIST Cybersecurity Framework (CSF) as the measuring stick to provide global insight into how organizations rate their overall cybersecurity maturity and practices. Here's what we learned.

**Larger organizations report more maturity than smaller organizations.**

**HOW DOES YOUR ORGANIZATION RATE?**

TAKE THE SURVEY NOW
RSA.COM/MATURITYSURVEY

**ORGANIZATION SIZE DOES MATTER**

Key Takeaways

74%

AT RISK

71%

AT RISK

77%

AT RISK

**GEOGRAPHY DOESN'T MATTER**

Organizations in EMEA reported the most mature security strategies with 29% ranked as developed or advantaged vs APJ at 26% and the Americas at 23%.

**ORGANIZATION SIZE DOES MATTER**

**WEED VARIABLE ACROSS INDUSTRY**

State of Capabilities

USING THE NIST CYBERSECURITY FRAMEWORK

The damage imposed by cyber security breaches and attacks is constantly increasing, particularly in the area of advanced threat attacks. Therefore, effective protection and response mechanisms are needed. To that end, the Secure Cyber Nation Index (SCNI) offers a comprehensive picture of the different aspects of digital safety, including the business environment, government policies, and public awareness.

DAMAGING SECURITY INCIDENTS ARE THE MAIN FACTOR DRIVING ACTION AND CULTURE CHANGE

35% DEVELOPED OR ADVANTAGED

21% DEVELOPED OR ADVANTAGED

65% MORE MATURE

21 OR MORE INCIDENTS

1-10 INCIDENTS

AS A RESULT, MOST ORGANIZATIONS REMAIN CHALLENGED WITH REGARD TO THEIR SECURITY AND RISK POSTURE

75% AT RISK

7% ADVANTAGED

EXTREMELY WELL POSITIONED TO DEFEND ITS IT ASSETS AGAINST ADVANCED THREATS

18% DEVELOPED

HAS A WELL-DEVELOPED SECURITY PROGRAM AND IS WELL POSITIONED TO FURTHER IMPROVE ITS EFFECTIVENESS

41% FUNCTIONAL IMPLEMENTING SOME SECURITY BEST PRACTICES, MAKING PROGRESS

27% DEFICIENT PROVIDING INADEQUATE SECURITY PROTECTION

7% NEGLIGENT FALLING WELL SHORT OF BEST SECURITY PRACTICES

OVERALL CAPABILITIES AMONG ALL COMPANIES

INCIDENTS IN THE LAST 12 MONTHS

A poverty gap has emerged between companies who are more mature and those who are not.

INCIDENT RESPONSE AND RISK IDENTIFICATION ARE UNDERDEVELOPED The lack of these capabilities prevents organizations from reactively minimizing business impact of incidents or proactively prioritizing areas of improvement.

**CRITICAL ASSETS**

**ABILITY TO CATALOG, ASSESS, AND MITIGATE CYBER RISK PRIORITIZE, AND COMMUNICATE RESPONSES, COORDINATE INCIDENT RESPONSE ACTIVITY WITH INTERNAL AND EXTERNAL STAKEHOLDERS**

42% CAPABILITY IS AD HOC OR NON-EXISTENT

45% CAPABILITY IS AD HOC OR NON-EXISTENT

42% CAPABILITY IS AD HOC OR NON-EXISTENT

45% CAPABILITY IS AD HOC OR NON-EXISTENT

**40%**

RESPOND

**IDENTIFY**

**CRITICAL ASSETS**

**AP**

**P**

**S**

**BUILD SYSTEMS AND INTELLIGENCE TO RECOGNIZE POTENTIAL CYBERSECURITY EVENTS AS THEY HAPPEN.**

**IDENTIFY ASSETS THAT SUPPORT CRITICAL BUSINESS FUNCTIONS, ASSESS RISK, AND PRIORITIZE SECURITY EFFORTS.**

**BUILD AND MAINTAIN TECHNOLOGY, PROCESS-ES, AND PROCEDURES TO SECURE AND CONTROL ACCESS TO CRITICAL INFORMATION.**

**CONTAIN AND LIMIT THE EFFECTS OF CYBERSECURITY EVENTS THROUGH PLANNING AND ACTION.**

**RESTORE AFFECTED SYSTEMS AND SERVICES TO QUICKLY RETURN TO NORMAL BUSINESS OPERATIONS.**