RSA Cybersecurity Poverty Index™

2016

RSA

Overview

Welcome to RSA's second annual Cybersecurity Poverty Index™.

The RSA Cybersecurity Poverty Index is the result of an annual maturity self-assessment completed by organizations of all sizes, industries, and geographies across the globe. The assessment was created using the NIST Cybersecurity Framework (CSF). This year's assessment was completed by 878 respondents across 81 countries. Of the 878 respondents, 438 are from the Americas, 240 from EMEA, and 200 from APJ.

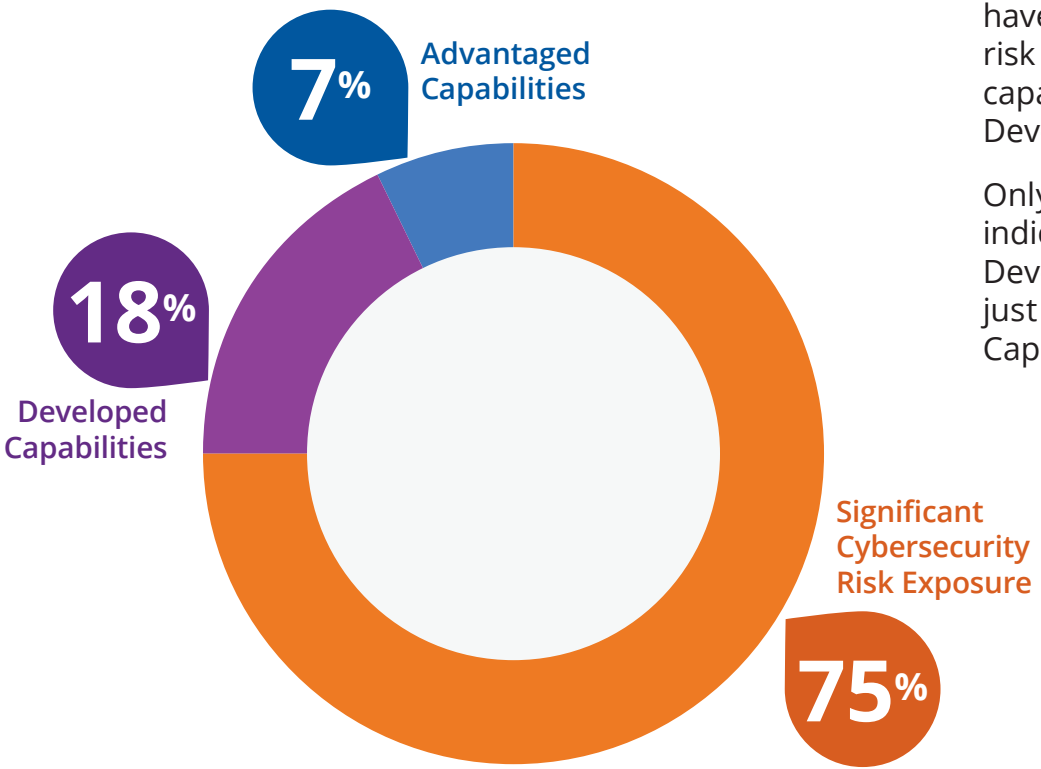
Our goal in creating and conducting this global research initiative is two-fold. First, we want to provide a measure of the risk management and information security capabilities of the global population. As an industry leader and authority, we are often asked "why do security incidents that negatively impact organizations continue to occur?" We believe that a fundamental gap in capability is a major contributor, and hope that this research can illuminate and quantify that gap. Second, we wish to give organizations a way to benchmark their capabilities against peers and provide a globally recognized practical standard, with an eye towards identifying areas for improvement.

Methodology

Organizations rated their own capabilities by responding to 18 questions that covered the five key functions outlined by the CSF: **Identify, Protect, Detect, Respond**, and **Recover.**

Respondents rated capabilities using a 5 point scale	Each respondent received an overall score for their program based on their responses.
1. **Not Currently Done** My organization does not currently do this. 2. **Ad Hoc** My organization handles this in an ad hoc or case-by-case manner. Our practices in this area are not formalized and are most often handled in a reactive manner without using repeatable processes. 3. **Progressing** My organization has progressed from a purely ad hoc or case-by-case approach in this area, but is in the early stages of formalizing its practices and executing them on an organization-wide basis. 4. **Mature** My organization's security practices in this area are mature and are generally consistently repeated on an organization-wide basis. 5. **Mastered** My organization's security practices in this area are highly mature, adaptive, risk focused, enterprise in scope, and almost always based-on lessons learned from internal experiences, quantitative metrics, or externally sourced best practices.	• **Negligent** - Falling well short of best security practices and thus neglecting its responsibility to properly protect its IT assets. • **Deficient** - Providing inadequate security protection and thus falling short in its responsibility to protect its IT assets. • **Functional** - Has generally implemented some security best practices and thus making progress in providing sufficient protection for its IT assets. • **Developed** - Has a well-developed security program and is well positioned to further improve its effectiveness. • **Advantaged** - Has a superior security program and is extremely well positioned to defend its IT assets against advanced threats.

Overall

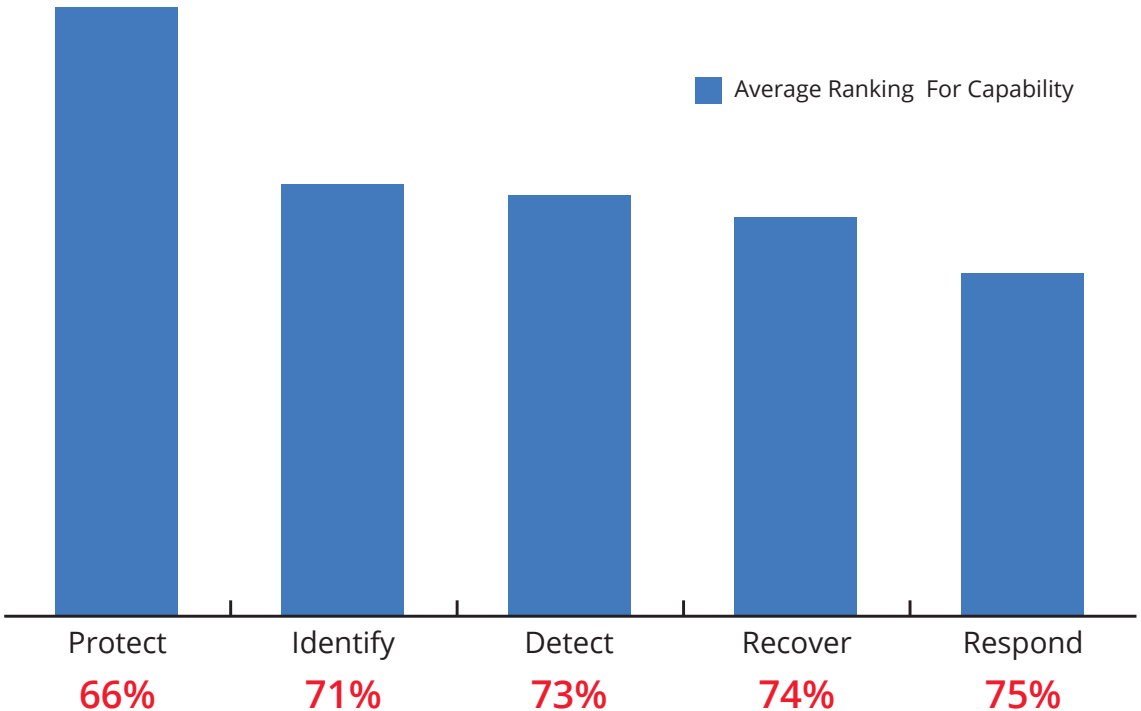


The overall survey results found that ***75%*** of respondents have significant cybersecurity risk exposure (with overall capabilities falling below the Developed category).

Only ***18%*** of respondents indicated that they have Developed Capabilities, and just ***7%*** have Advantaged Capabilities.

By Type of Capability

The strongest reported maturity levels were in the area of Protection - this function forms the basis of conventional security doctrine that is proving less and less effective over time in the face of advanced threats. Response, the function which, along with Detection, forms the backbone of today's effective security strategies, ranked last in maturity.

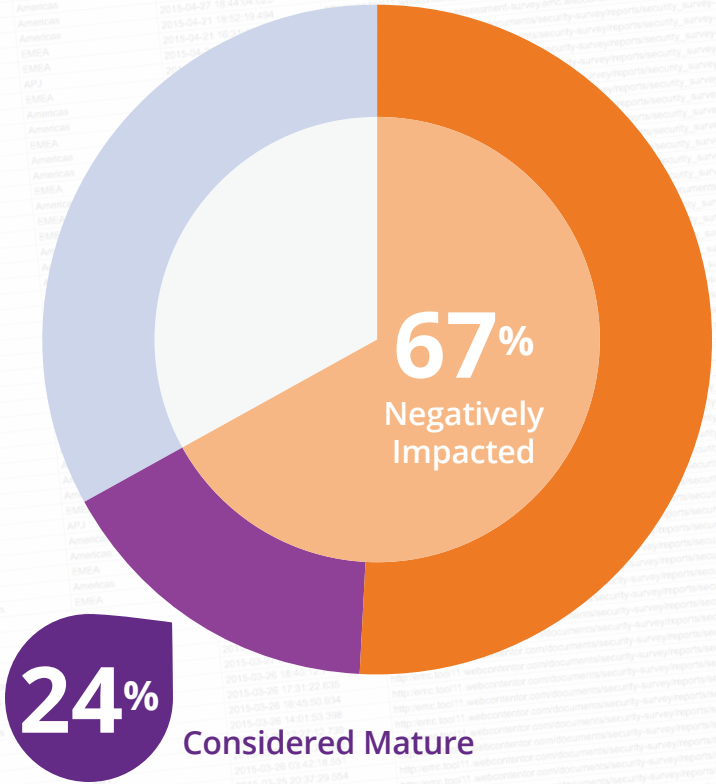


% of respondents with inadequate levels of capability within the function

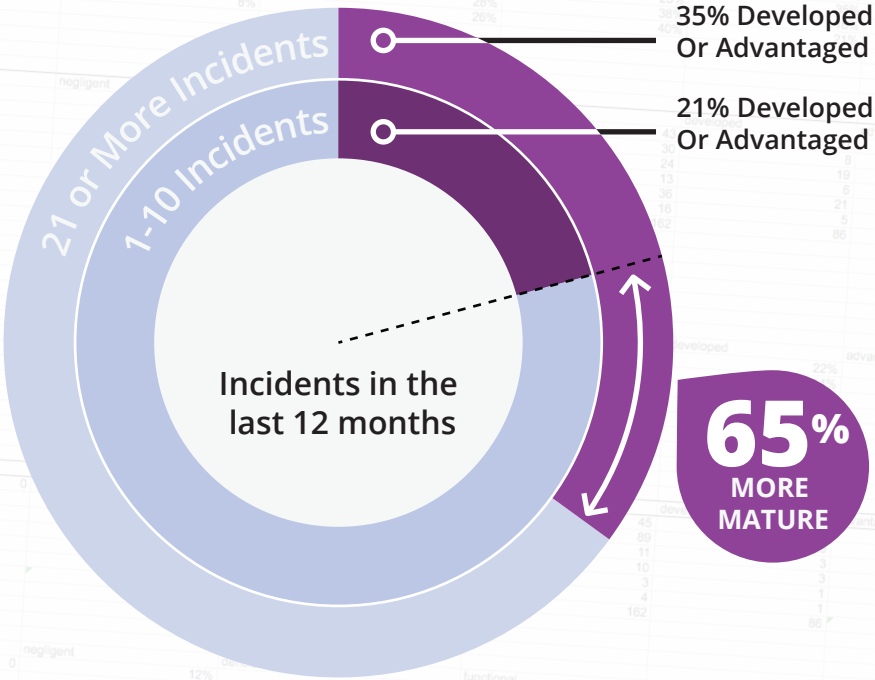
By Number of Incidents

67% of respondents had incidents that negatively impacted their business operations in the last 12 months, but ***only 24% of those were considered mature in their security strategy.***

This inidicates an inability to meaningfully improve maturity to reduce risk, and confirms the continued capability of adversaries to exploit gaps in conventional defense strategies.



By Number of Incidents



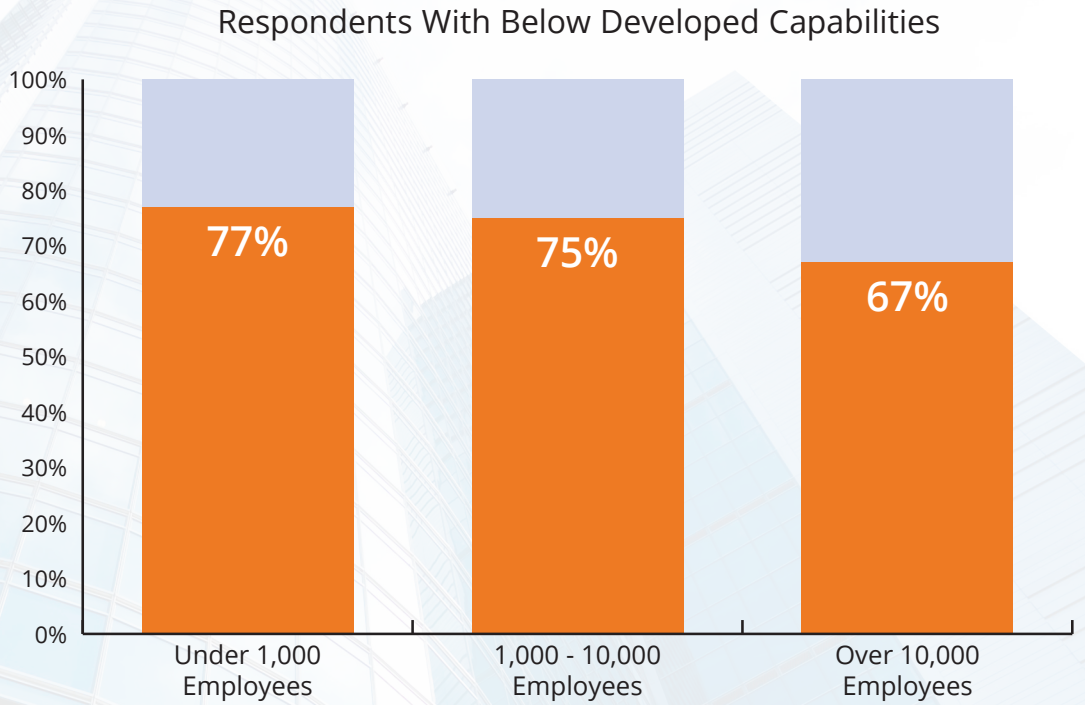
Organizations that deal with security incidents more regularly are significantly more mature than their peers.

Organizations who reported 21 or more security incidents in the last 12 months are ***65% more likely*** to have "Developed" or "Advantaged" overall capabilities than those reporting 1-10 incidents.

By Size of Organization

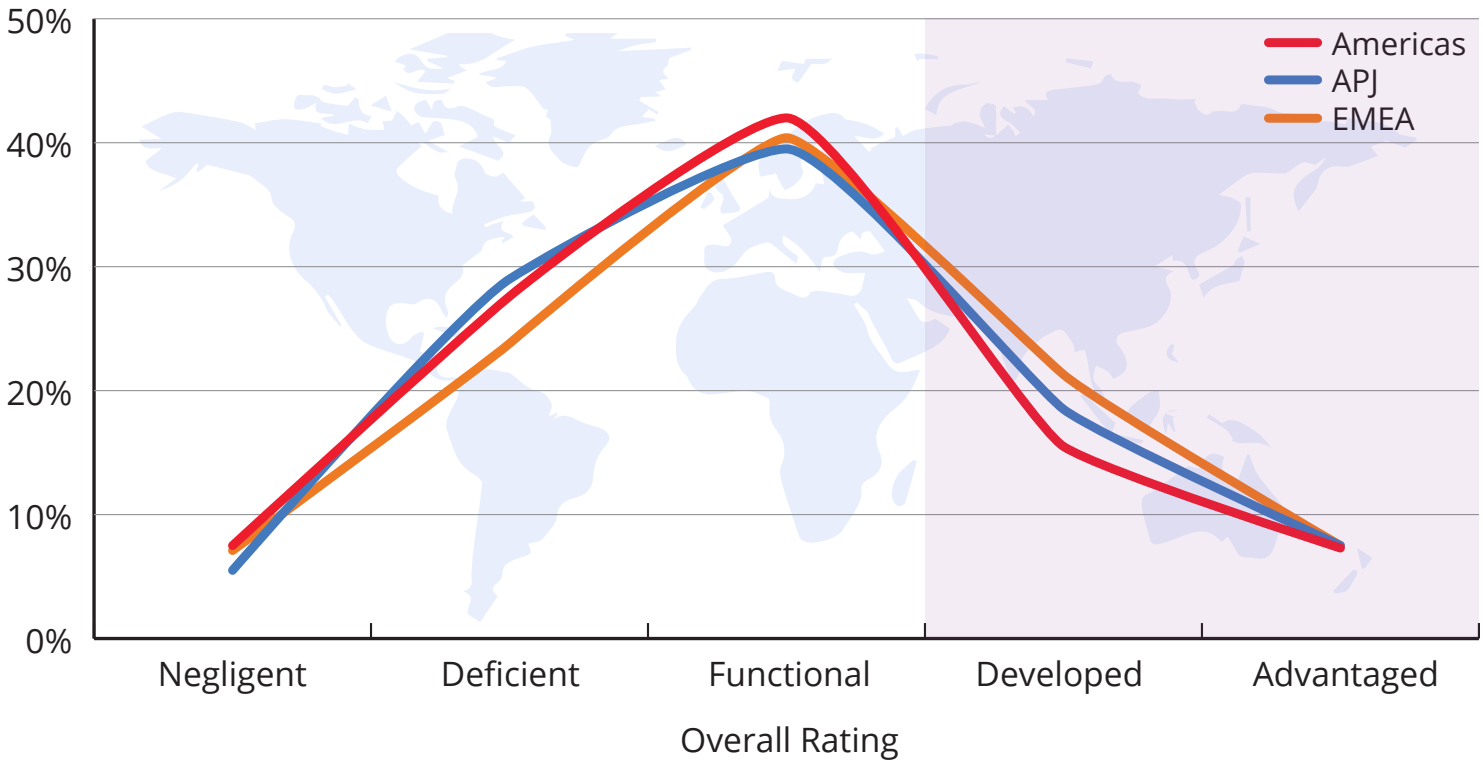
Overall, smaller organizations are less mature than larger organizations.

67% of respondents surveyed with more than 10,000+ employees are not well prepared for today's threats (ranking below Developed in overall maturity).



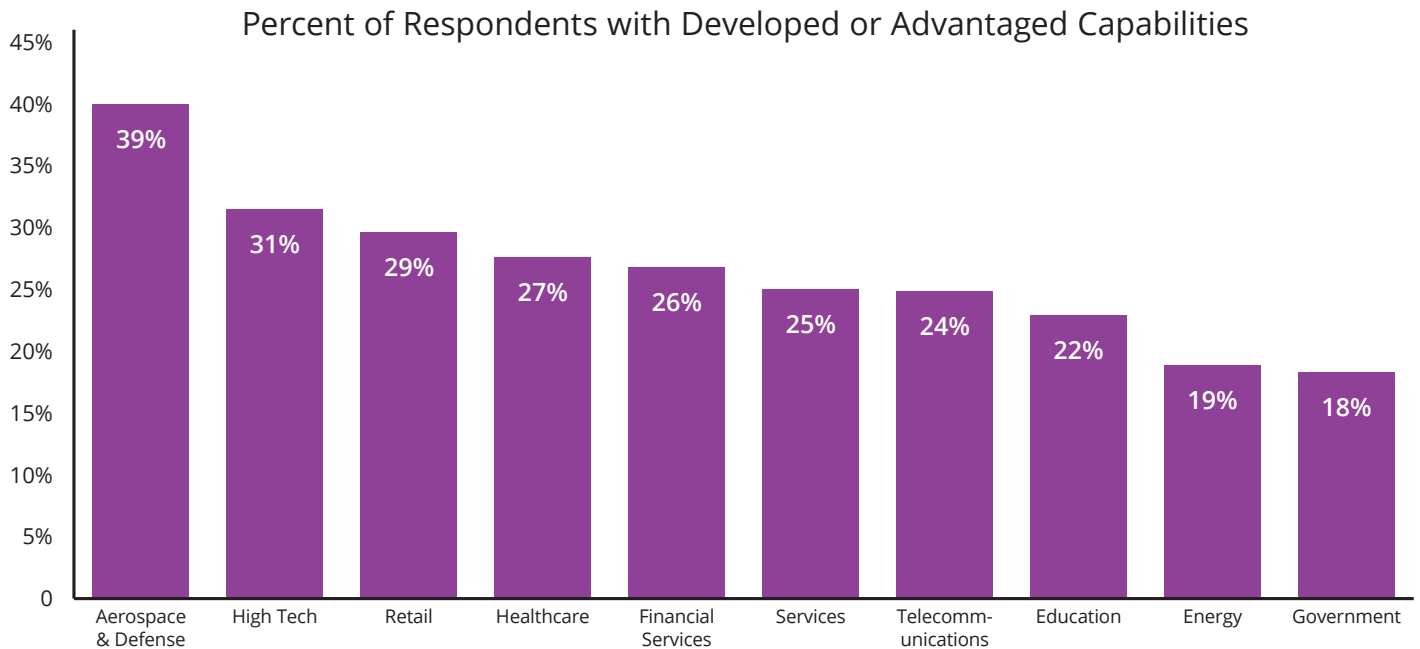
By Geography

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%***.



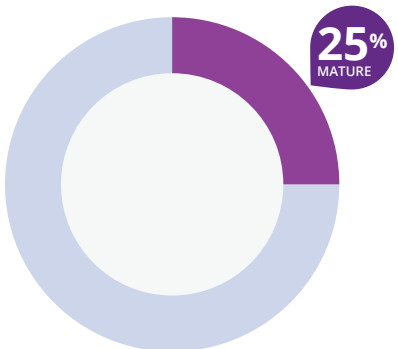
By Vertical Industry

Organizations in the Aerospace and Defense industry by far reported the highest level of maturity with respondents having developed or advantaged capabilities. Government and Energy ranked lowest across industries in the survey.



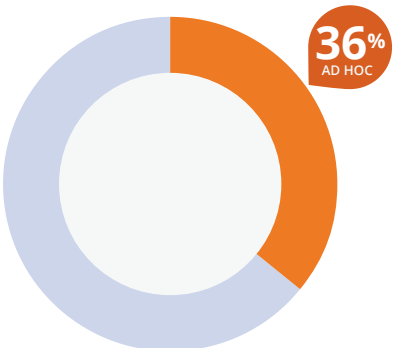
Note: Data limited to industries with at least 30 respondents

Detail on Individual Capabilities



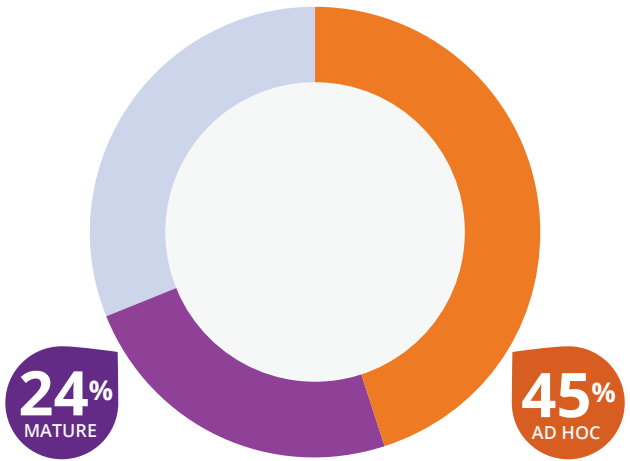
Capabilities for **incident response** and **recovery** were consistently seen as underdeveloped, with an average of ***25% of respondents*** rating their capabilities as ***mature or mastered across the function.***

Capabilities to **detect** threats – "monitoring network, endpoint, server, and application activity to detect potential security issues" are generally immature and less developed than other capabilities, with ***36% of organizations*** in the survey describing their capabilities as either ***non-existent or ad hoc.***

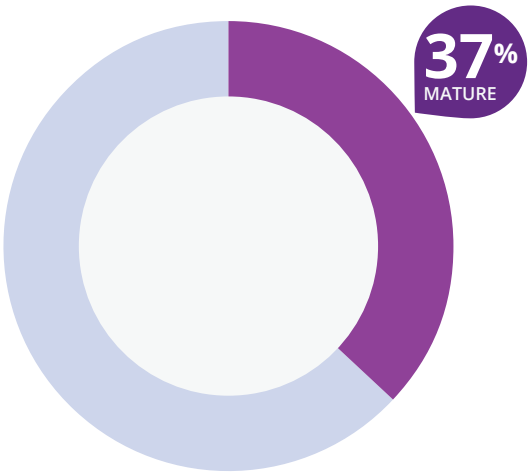


The challenges reported by respondents demonstrate why breaches continue to take so long to discover and consequently often result in significant damage or loss to the organization.

Detail on Individual Capabilities



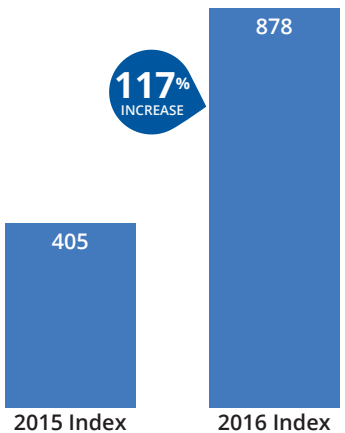
The least developed capability across the survey is an organization's **ability to catalog, assess, and mitigate risk.** ***45% of those surveyed*** described their capabilities in this area as ***non-existent or ad hoc,*** with only ***24%*** believing that they have ***mature or mastered capabilities*** in this domain.



IAM ("managing and governing identities and their access to IT resources") ranked as the most developed capability, with ***37% of respondents*** rating their capabilities as ***mature or mastered.***

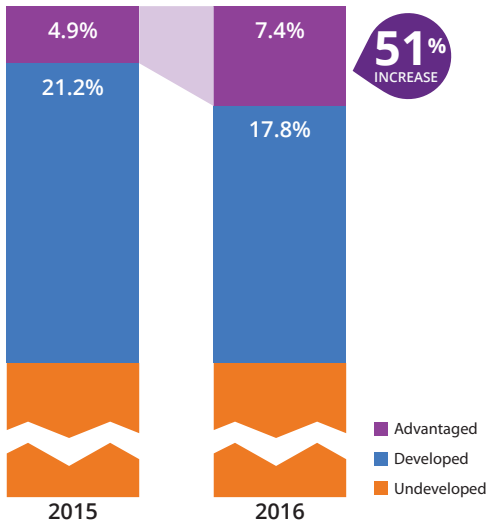
Year Over Year Comparison: Overall

Number of Respondents



The number of participants ***more than doubled*** from the 2015 Index to the 2016 Index.

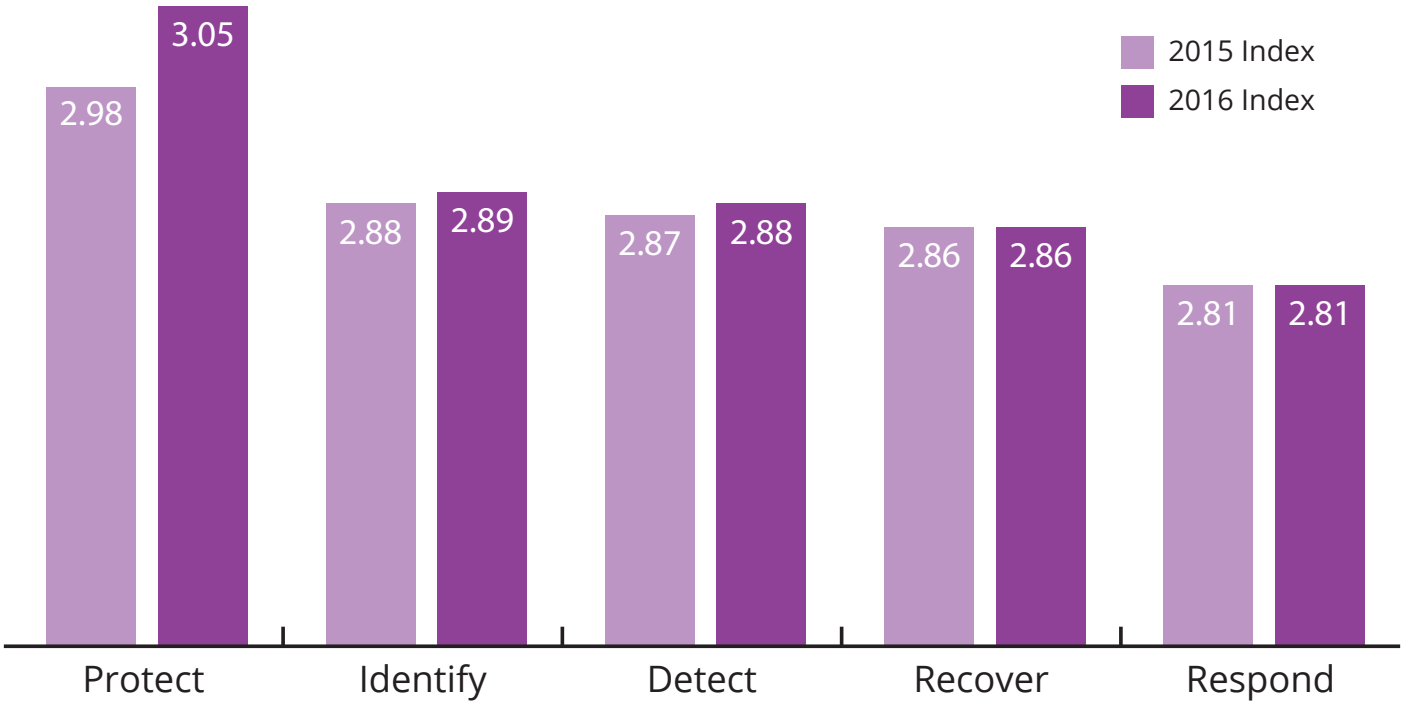
Maturity



The percentage of respondents reporting significant cybersecurity risk exposure remained near ***75%.*** Progress is reported within more mature organizations: the percentage of organizations reporting advantaged capabilities overall increased ***51%*** from our last index, from ***4.9%*** to ***7.4%.***

Year Over Year Comparison: Capabilities

While no category of capability declined from the previous Index, the CSF domain capability showing the greatest improvement from the last Index was Protect. The reported maturity across the remaining domains (Identify, Detect, Recover, Respond) either remained consistent, or increased only marginally.



Conclusion

The results speak for themselves. There is work to be done to improve risk management and cybersecurity capabilities regardless of company size, geography, or vertical industry.

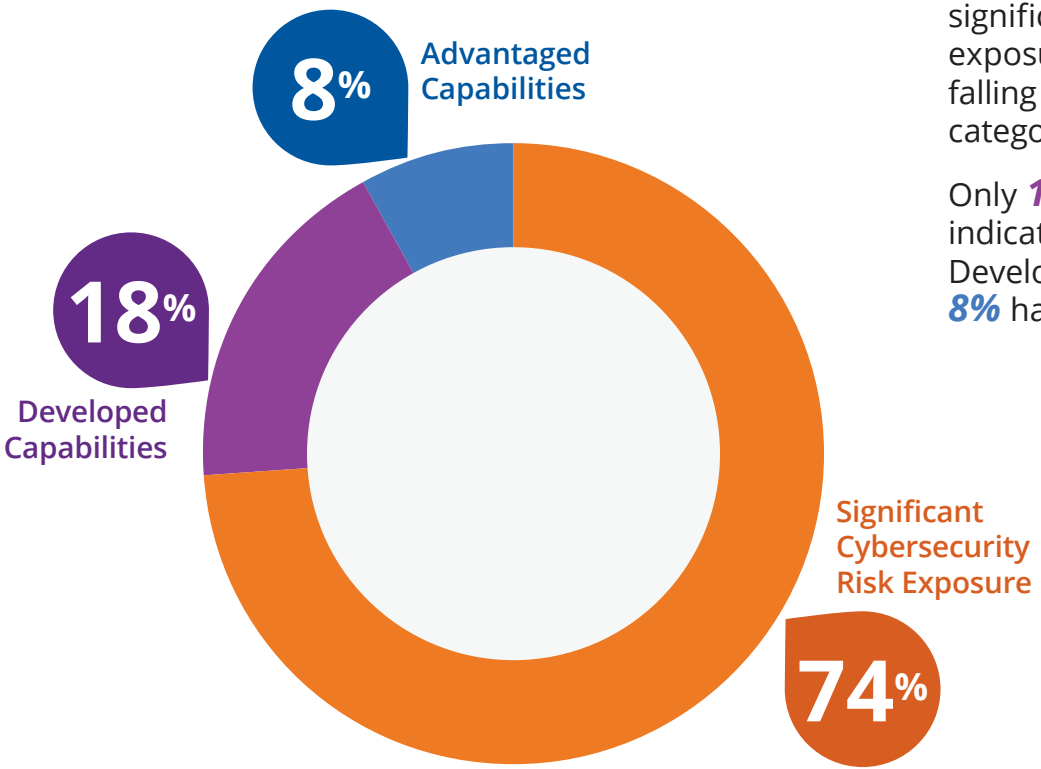
Two important findings stand out from the wealth of data. First, damaging security incidents are the main factor driving action and culture change. Effective Incident Response capabilities, which can help minimize the business impact of security incidents, are particularly underdeveloped. However, organizations that experience the most security incidents are significantly more likely to have developed or advantaged overall capabilities. Once organizations experience an incident that negatively impacts their operations, they strive to improve their capabilities and maturity at a greater pace to mitigate the effects of (inevitable) future incidents. As a result, a greater disparity has emerged between those organizations who are more mature and those who are not. Second, organizations struggle to take proactive steps to improve their cybersecurity and risk posture because they struggle to understand cyber risk and how it will impact their operations. The least developed capability across the survey is an organization's ability to catalog, assess, and mitigate risk. The inability to assess cyber risk and calculate cyber risk appetite makes it impossible to prioritize areas of mitigation and investment.

If you completed the assessment this year, we thank you for your participation and look forward to your continued input in future years. If you did not participate, we encourage you to complete the survey and obtain a benchmark that can help you plan for advancing your organization's capabilities.

Take the survey today at rsa.com/maturitysurvey.

APJ Addendum

APJ: Overall

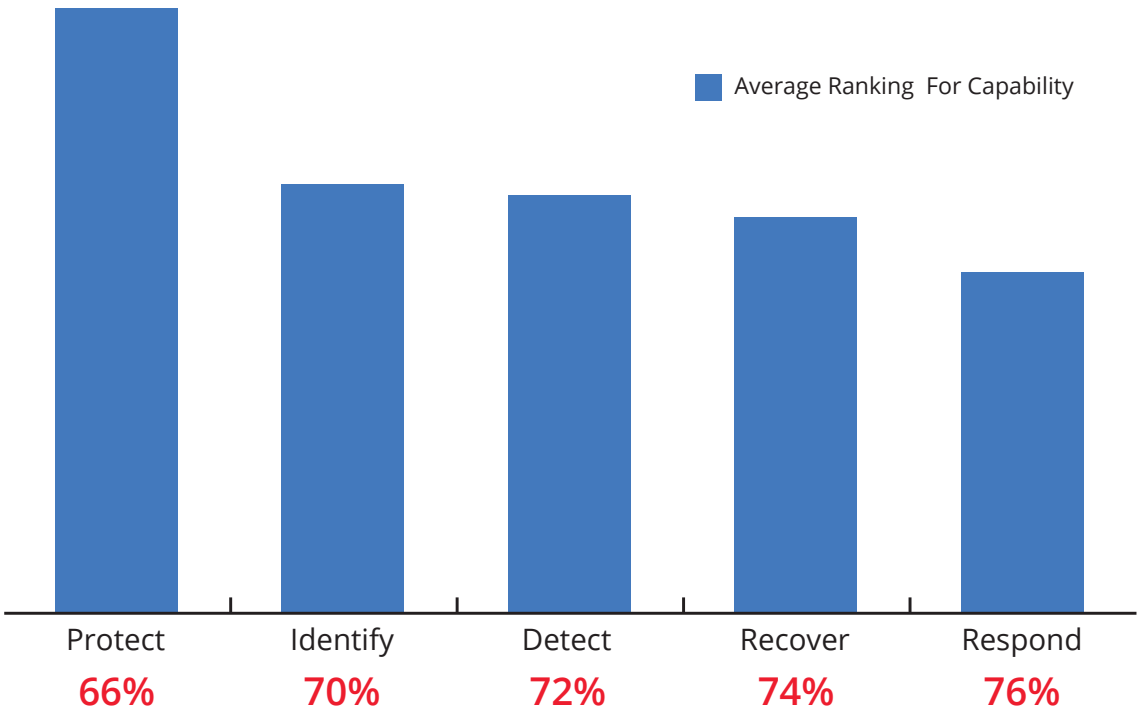


The overall survey results found that ***74%*** of respondents have significant cybersecurity risk exposure (with overall capabilities falling below the Developed category).

Only ***18%*** of respondents indicated that they have Developed Capabilities, and just ***8%*** have Advantaged Capabilities.

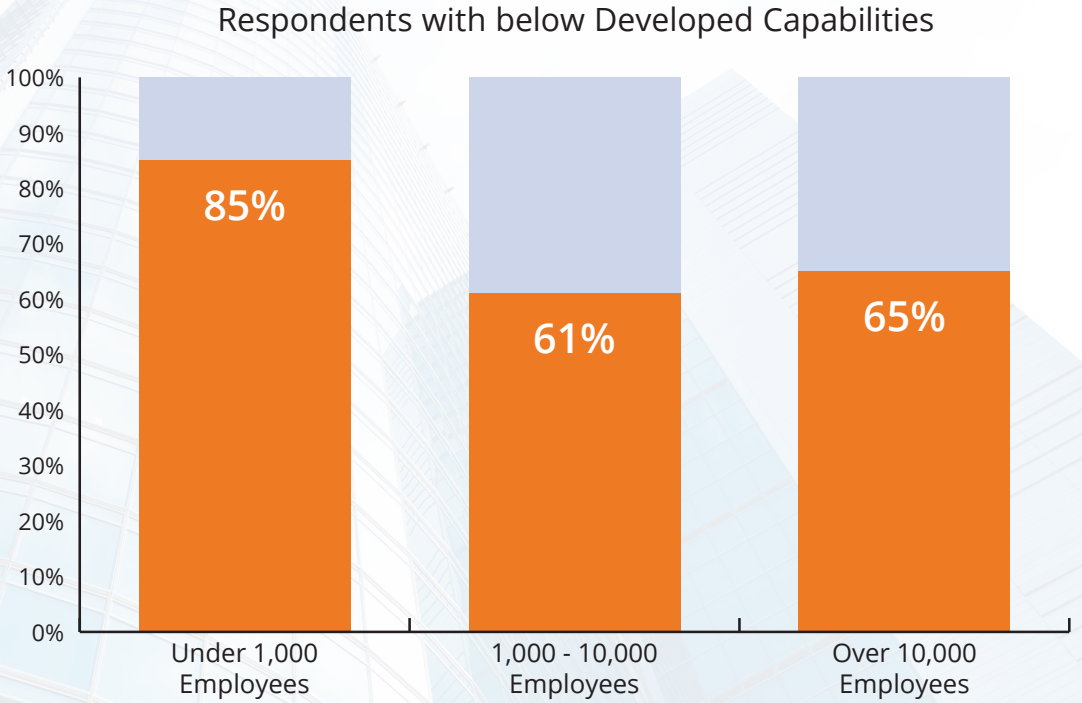
APJ: By Type of Capability

In APJ, the strongest reported maturity levels reported were in the area of Protection. Response ranked last in maturity across functions.



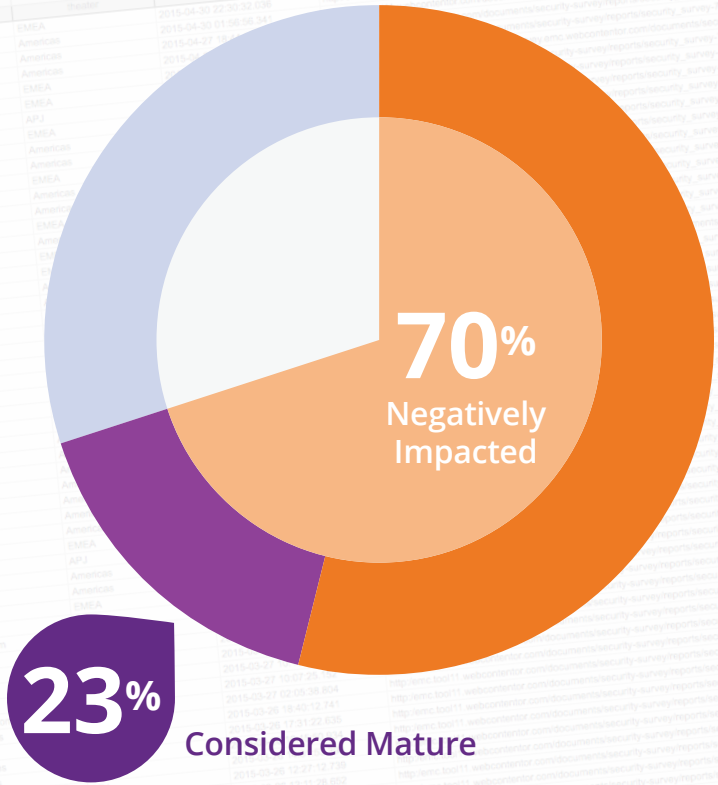
APJ: By Size of Organization

85% of organizations surveyed with under 1,000 employees are not well prepared for today's threats (ranking below Developed in overall maturity).



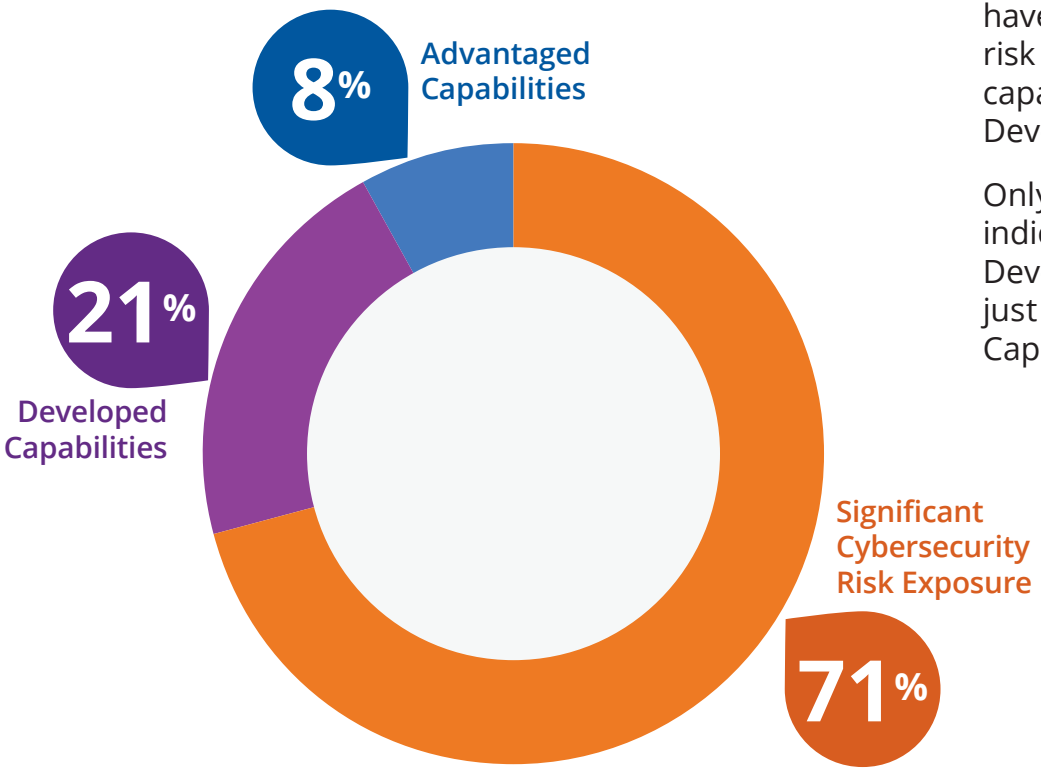
APJ: By Number of Incidents

In APJ, ***70%*** of respondents had incidents that negatively impacted their business operations in the last 12 months, but ***only 23%*** of those were considered mature in their security strategy.



EMEA Addendum

EMEA: Overall

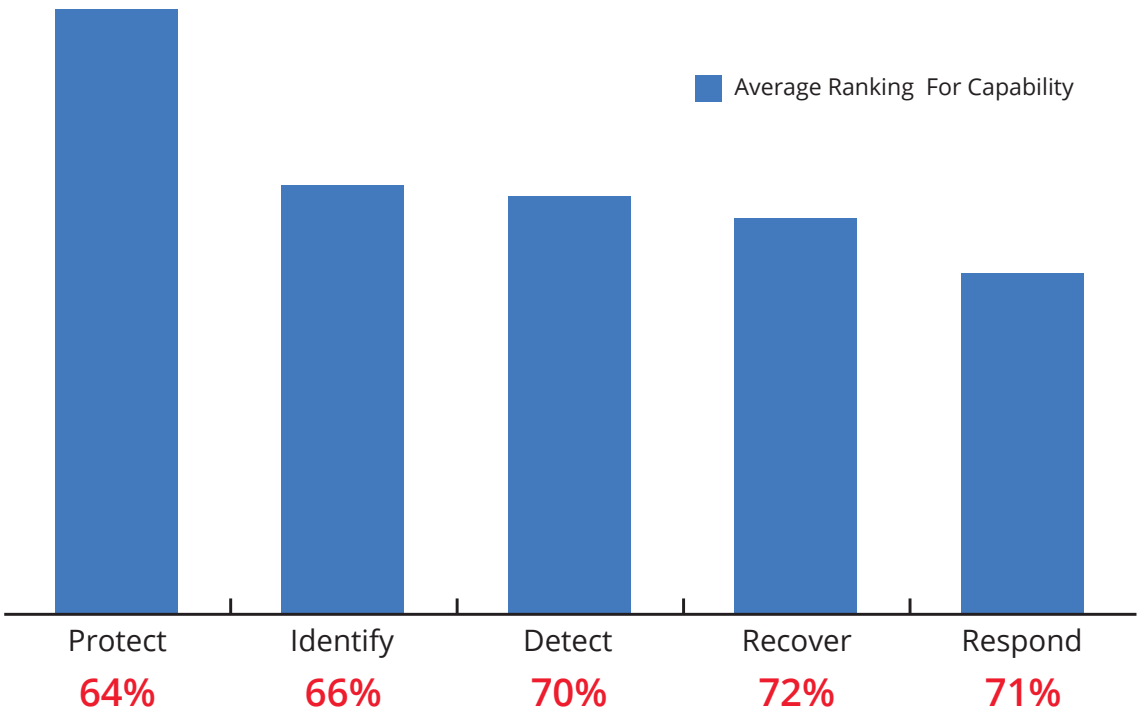


The overall survey results found that ***71%*** of respondents have significant cybersecurity risk exposure (with overall capabilities falling below the Developed category).

Only ***21%*** of respondents indicated that they have Developed Capabilities, and just ***8%*** have Advantaged Capabilities.

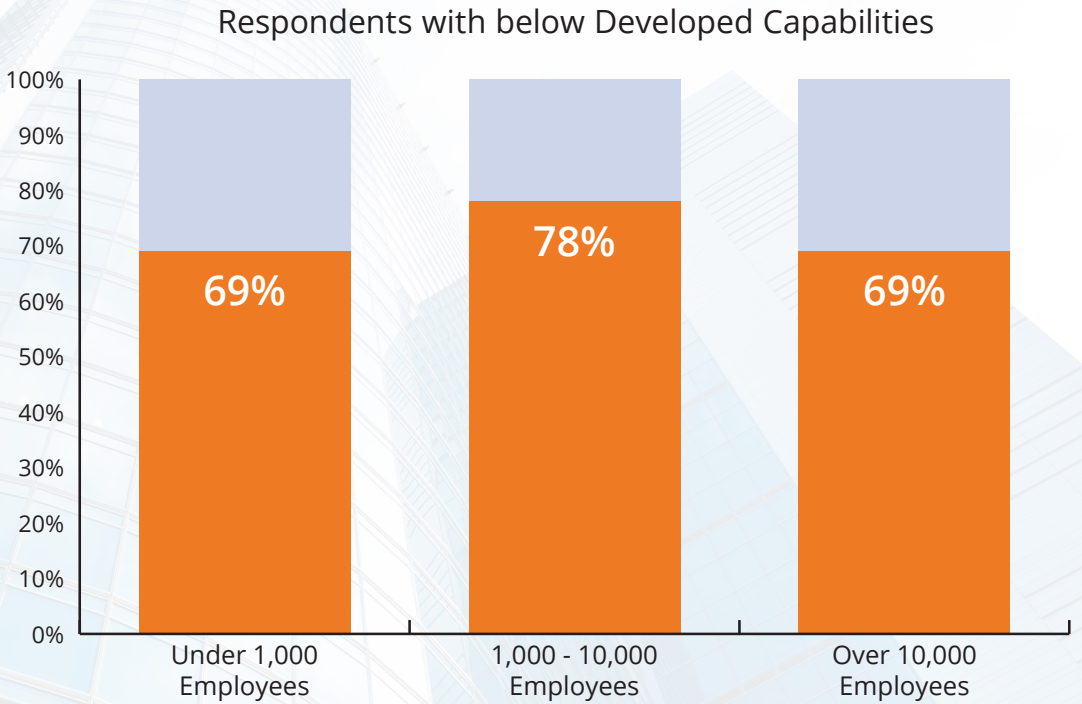
EMEA: By Capability

In EMEA, the strongest reported maturity levels reported were in the area of Protection. Response ranked last in maturity across functions.



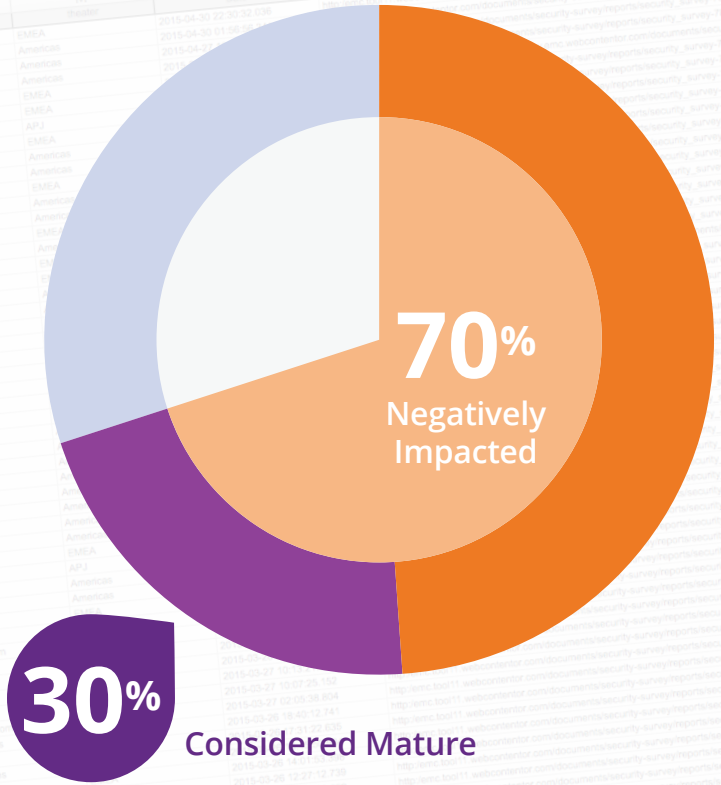
EMEA: Size of Organization

69% of organizations surveyed with under 1,000 employees are not well prepared for today's threats (ranking below Developed in overall maturity).



EMEA: By Number of Incidents

70% of respondents had incidents that negatively impacted their business operations in the last 12 months, but ***only 30%*** of those were considered mature in their security strategy.



RSA