

# CYBER RISK INDEX (CRI)

With cyberattacks a constant threat, it's crucial for companies to focus on assessing, detecting, preventing, and responding to today's cyber threats. In this iteration of the CRI, performed in 2020, Trend Micro and Ponemon Institute conducted research among IT managers across Europe, Asia-Pacific, and the USA, using the findings to create a comprehensive index to assess an organization's cyber risk maturity level. Each region showed an elevated risk level, contributing to an overall elevated risk level worldwide.

## Current industry average index:

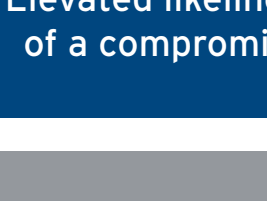
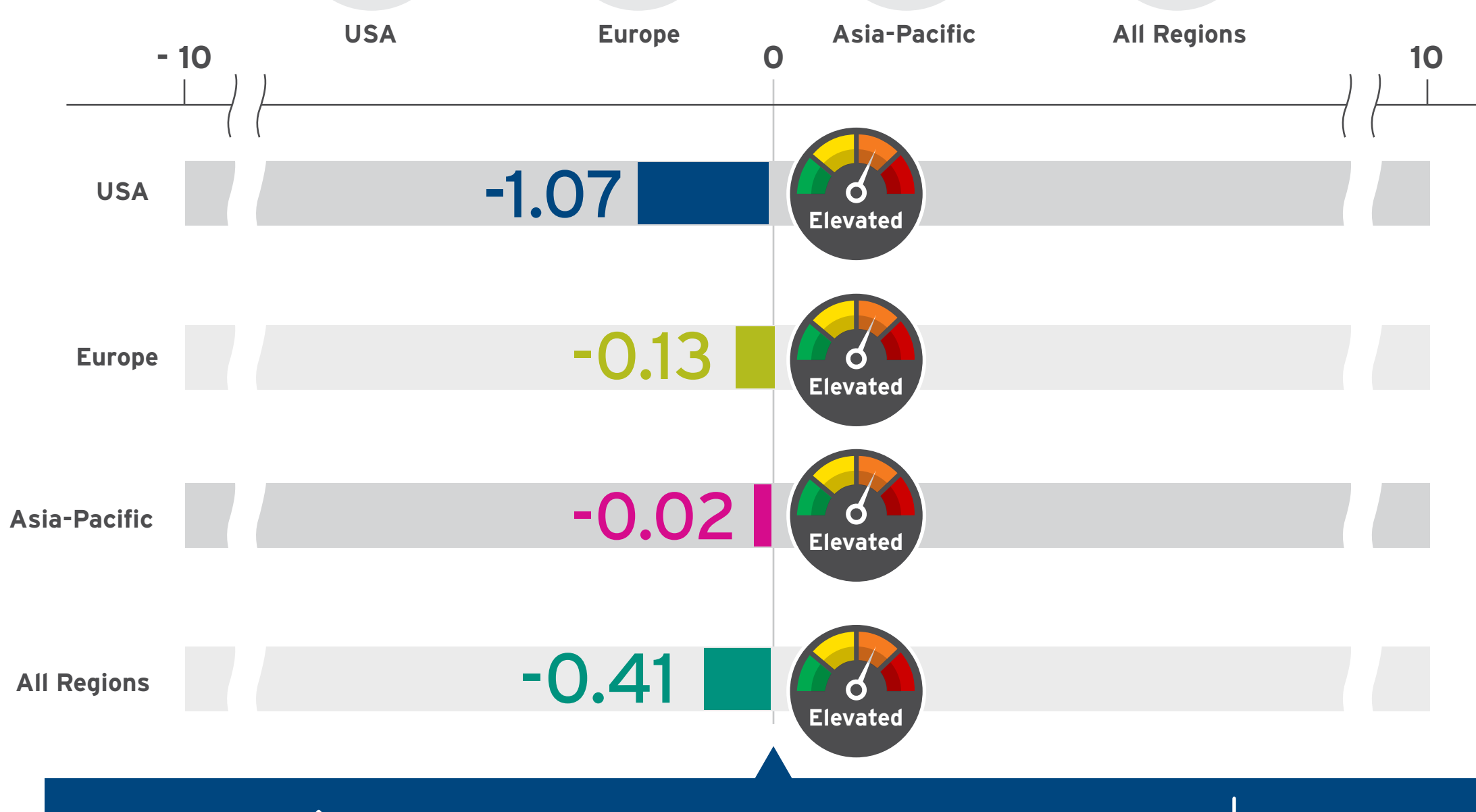


## Top risk factors associated with responses from those surveyed in the 2H'20 CRI



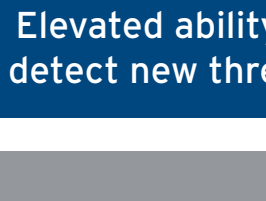
## Cyber Risk Index

This index measures the difference between the Cyber Preparedness Index and the Cyber Threat Index. In other words, the divide between an organization's current security posture and their likelihood of being attacked.



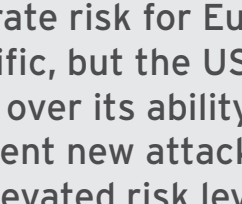
Elevated likelihood of a compromise

The USA region has the highest overall risk, due to less preparedness than the other two regions.

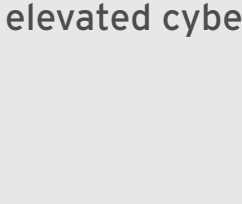


Elevated ability to detect new threats

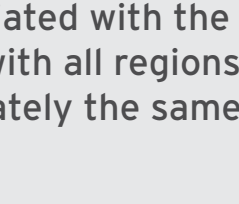
## Overall



The Cyber Preparedness Index was at a moderate risk for Europe and Asia-Pacific, but the USA showed concerns over its ability to detect and prevent new attacks with an elevated risk level.



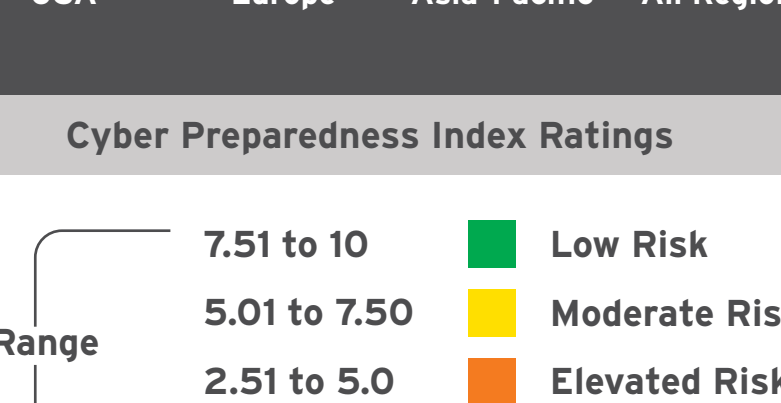
Overall, all organizations are at an elevated cyber risk.



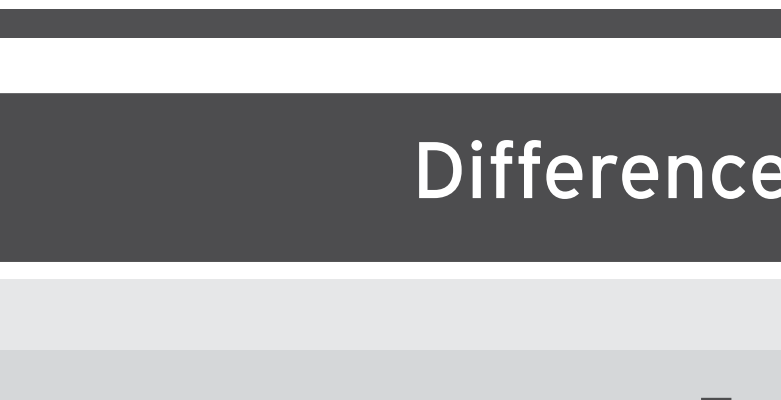
All organizations show an elevated risk associated with the Cyber Threat Index, with all regions exhibiting approximately the same level of risk.

## Cyber Preparedness Index

Lower number, higher risk

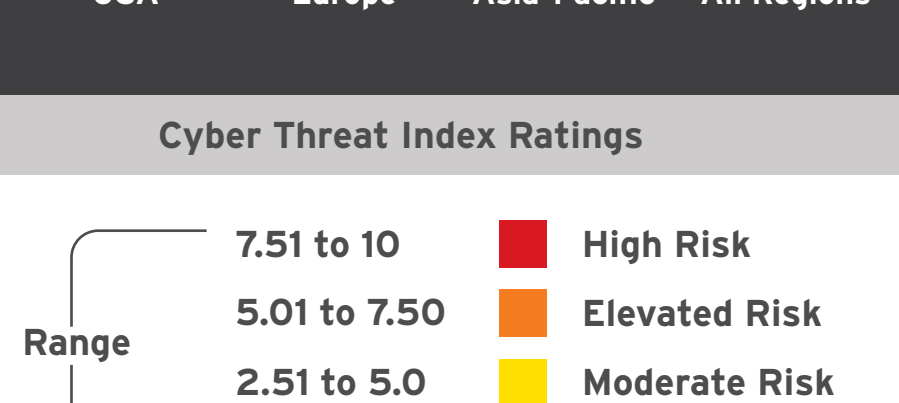


### Cyber Preparedness Index Ratings

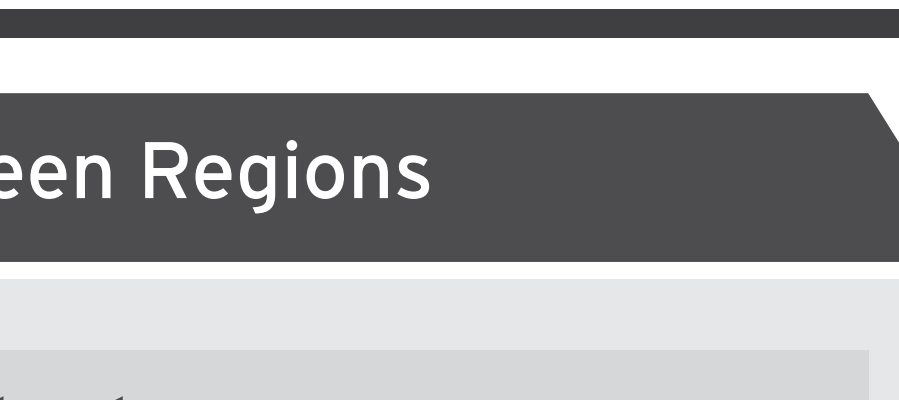


## Cyber Threat Index

Higher number, higher risk

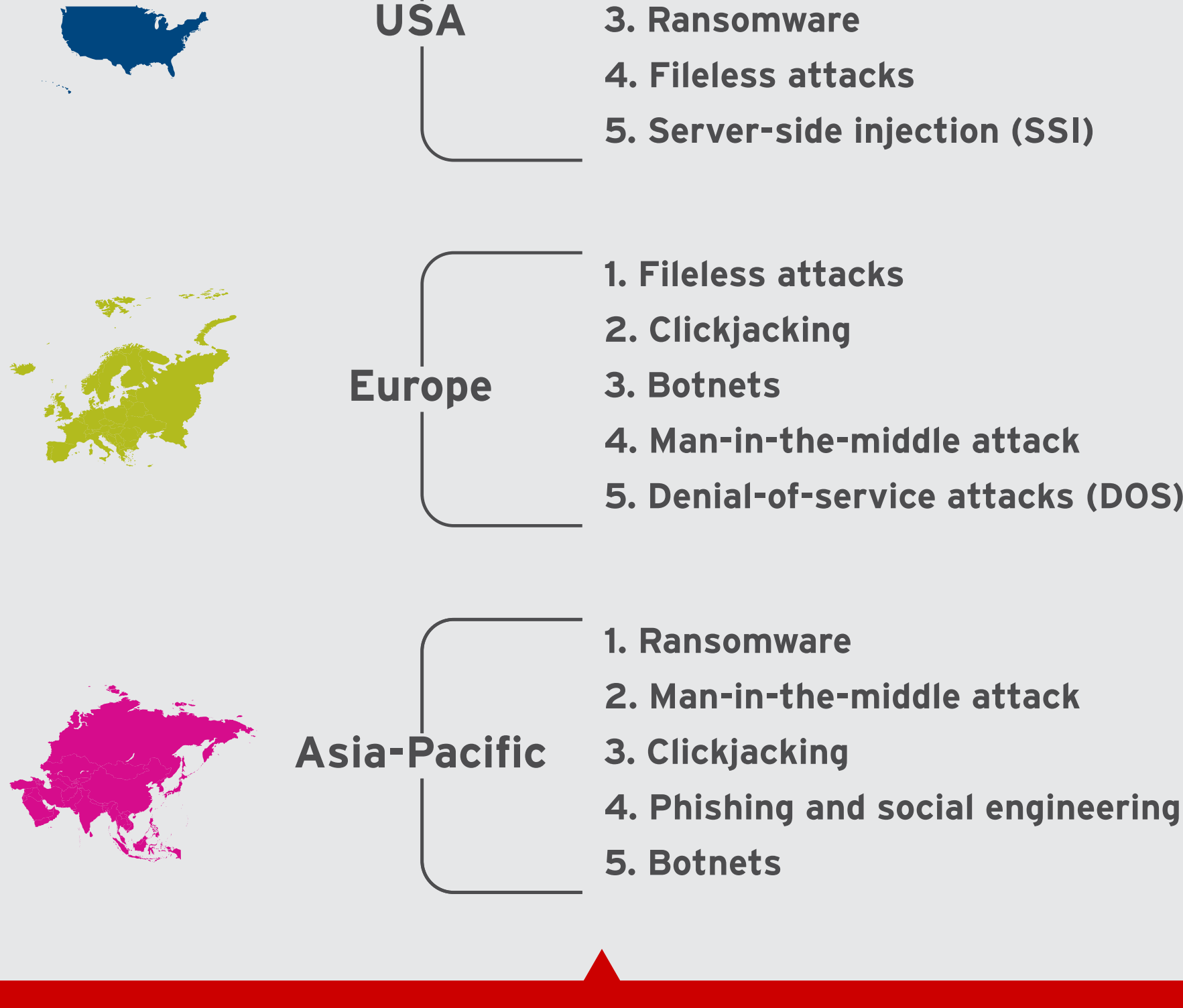


### Cyber Threat Index Ratings



## Differences Between Regions

### Top 5 cyber threats



Clickjacking is the only threat all three regions included.

## These were the top risks to infrastructure across all three regional respondents:

- Organizational misalignment and complexity
- Cloud computing infrastructure and providers

This showcases the challenges organizations are having to deal with because of the many changes we're seeing within the infrastructure, including new cloud implementations.

## Likelihood of a successful cyberattack

Across the three regions, respondents appear to be concerned they will be successfully attacked in the next 12 months. **9 of 10 in the USA, 8 of 10 in Europe, and 7 of 10 in Asia-Pacific** are somewhat to very likely to be compromised in the next 12 months.

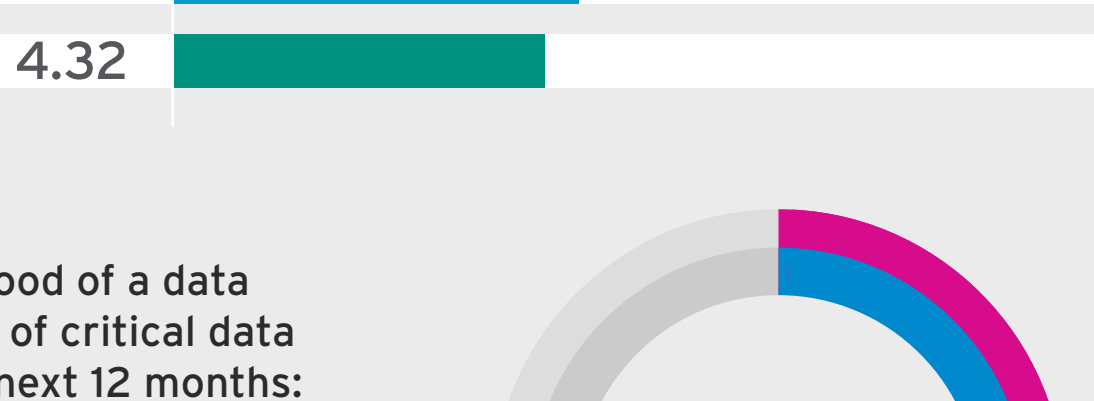


## Sample Survey Data

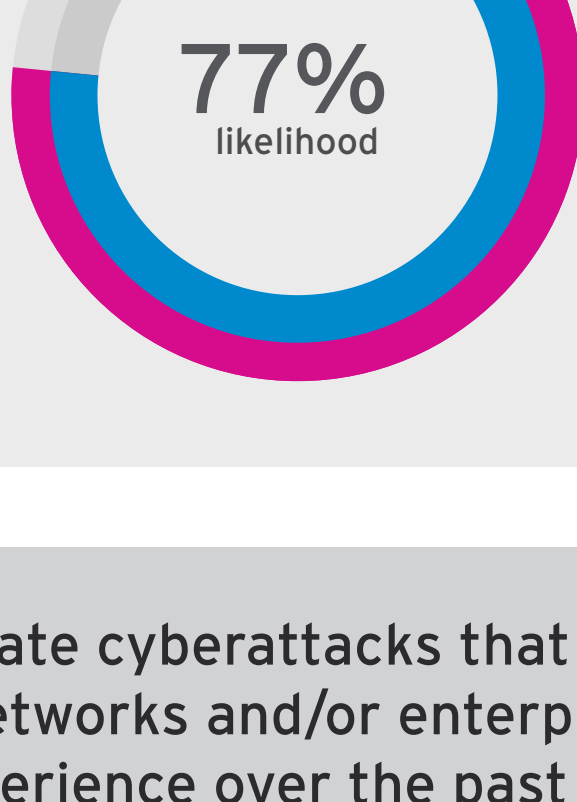
Several key survey questions were asked to IT managers to measure important aspects of their companies' cybersecurity posture. Here's a sampling of the survey's more revealing questions.

- USA
- Europe
- Asia-Pacific
- All Regions

### 1 Is your organization well-prepared to deal with data breaches and cybersecurity exploits? (Lower number means less prepared)



Likelihood of a data breach of critical data (IP) in next 12 months:



### Takeaway

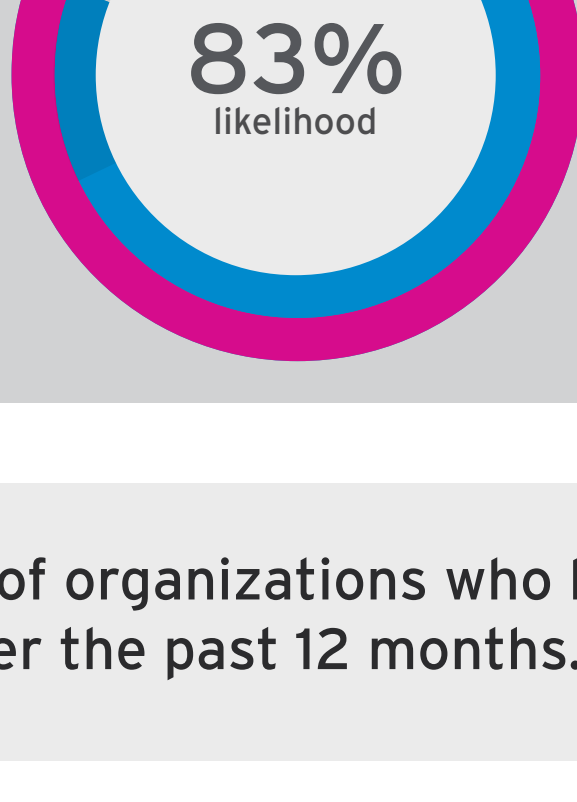
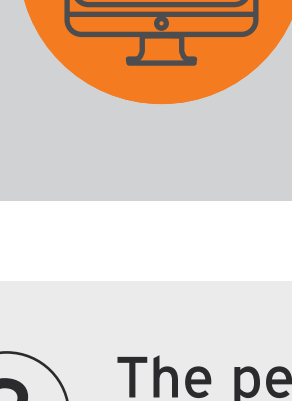


With nearly **4 out of 5** surveyed saying a breach of critical data is likely in the next 12 months, and a lack of preparedness to deal with an attack, organizations should rethink their current security strategy.

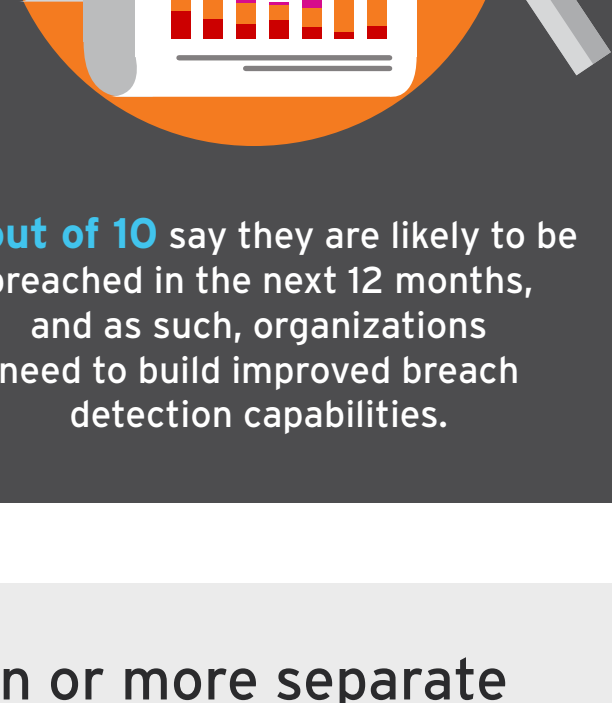
### 2 How many separate cyberattacks that infiltrated your organization's networks and/or enterprise systems did your organization experience over the past 12 months? Below shows percentage of those with one or more attacks.



Likelihood of one or more successful cyberattacks in the next 12 months:

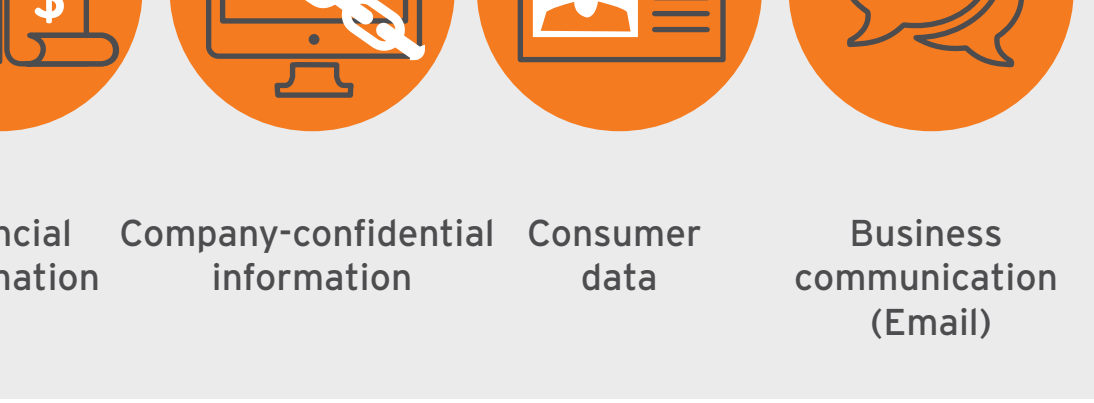


### Takeaway

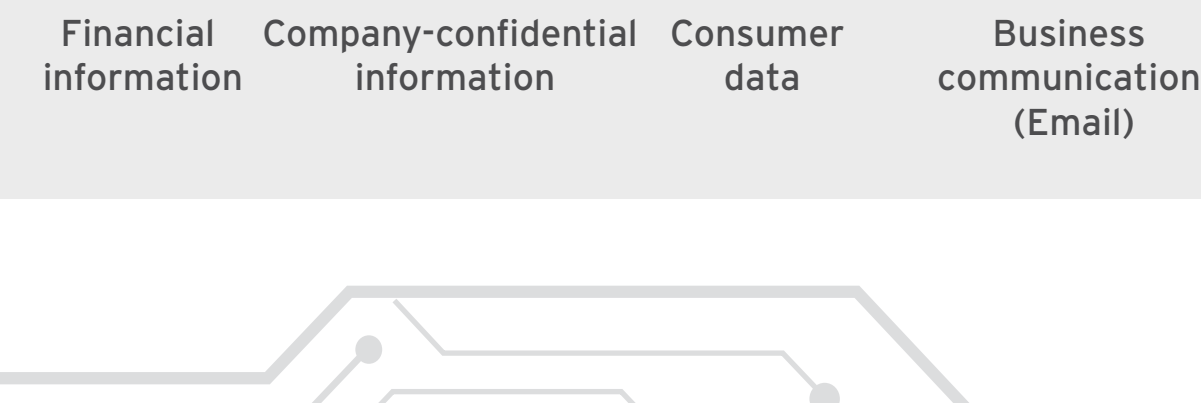


**8 out of 10** say they are likely to be breached in the next 12 months, and as such, organizations need to build improved breach detection capabilities.

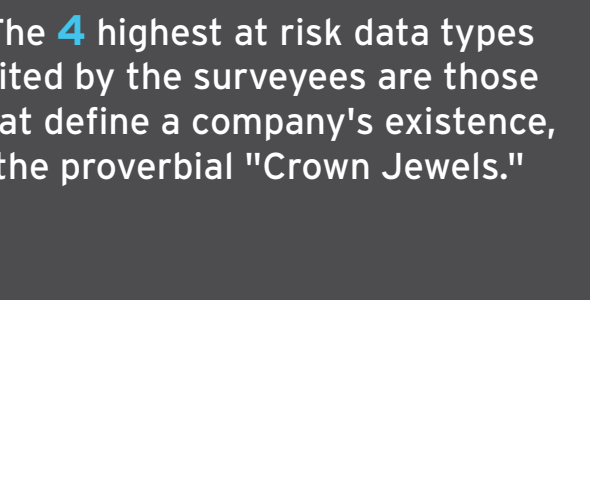
### 3 The percentage of organizations who had seven or more separate cyberattacks over the past 12 months.



The top four data types at highest risk of loss or theft are:



### Takeaway



The **4** highest at risk data types cited by the surveyees are those that define a company's existence, the proverbial "Crown Jewels."