Human Factor Security Market: By security type; By Industry; By Geography - Forecast(2018-2024)

Human factor role in security is becoming prominent, as the techniques followed by cyber criminals are subsequently progressing rapidly.

HYDERABAD, TELANGANA, INDIA, September 11, 2018 /EINPresswire.com/ -- Although advances in technology have made everyday life enjoyable, yet it carries many risks. Human factor role in security is becoming prominent, as the techniques followed by cyber criminals are subsequently progressing rapidly.

Now a days, attackers are targeting on social awareness factors as they play a key role in successful security attacks, but same scenario is not valid in many cases as these attacks are not always responsible for the mistakes made by insiders. Social engineering techniques are also responsible for such attacks as they trap individually targeted users into making mistakes. They also provide way for cyber criminals to hack into an organisation, and regrettably far too many organisations are making it easy for them. The targeted cyber-attacks involve spear-phishing scams with emails containing malevolent attachments that can cause malware to be downloaded into personal devices. This helps attackers to access valuable information of an organization such as intellectual property and other sensitive information.

To access / purchase the full report browse the link below
https://industryarc.com/Report/18548/human-factor-security-market.html

Human action is responsible for about 24% of cyber-attacks according to the Data Security Incident Report in 2016. Therefore, organizations must constantly educate their employees to avoid such attacks. Employees present in an organization are primary links that attackers can target easily to breach an organization's secure data. Most of the employees are uninformed of security, and they don't really believe they could do something that is breaking security. In the virtual world, people in general don't prefer to update their knowledge about latest technologies and most of them are unaware about the way they become target to attackers.

Website application attack accounted around 16% of cyber-attacks followed by other attacks according to the Global Threat Intelligence Report in 2017. Earlier, attackers used to target individuals by sending phishing mails but now a days Short Message Service (SMS) or text scams are mounting quickly than the phishing scam. Many organizations prefer employees to bring their own devices to work which makes them curious to open messages or get on hyperlinks from their devices, resulting in Image result for SMiShing attacks. Moreover, social media phishing is widely seen in many organizations. In this attackers often take advantage of organization's customer service requests as it is an easy way to lure individuals to share their credentials.
According to the Identity Theft Resource Center, in 2017, in the US, cybercrime rate has increased in 2017 when compared to previous year. There were 1,579 data breaches in the U.S. in 2017. The key factor responsible for such an increase in crime rate is lack of knowledge to detect new security loopholes. Modern day technologies help in addressing many issues compared to old ones, but they have their own set of drawbacks.

Talk to one of our sales representative about the full report by providing your details in the below link:
https://industryarc.com/support.php?id=18548

According to the International Telecommunications Union (ITU), the global internet users has increased tremendously from 2010 to 2017. With the rise in internet users there are significant chances for growth in cybercrime respectively. Therefore, additional care must be taken while browsing internet to avoid becoming victim to cyber-attack. Although, technology helps in safeguarding and processing against potential threats, still, there is a possibility for an organization to become target to attacks due to a human error. Apart from concentrating on technology and processes organizations must educate employees and raise awareness regarding probable threats caused by carelessness and also to stem errors made through social engineering. For an organization to become successful it must focus on people, processes and technology in equal order. By following such procedures employees can tackle the threats they face and can become a key part in safe guarding the organization sensitive data. An organization can be at maximum peace without becoming target to attackers only if they constantly educate employees about new technologies, identification of sceptical communications and possible hazards.

What can you expect from the report?
The Human Factor Security Market Report is Prepared with the Main Agenda to Cover the following 20 points:

1. Market Size by Product Categories
2. Market trends
3. Manufacturer Landscape
4. Distributor Landscape
5. Pricing Analysis
6. Top 10 End user Analysis
7. Product Benchmarking
8. Product Developments
9. Mergers & Acquisition Analysis
10. Patent Analysis
11. Demand Analysis (By Revenue & Volume)
12. Country level Analysis (15+)
13. Competitor Analysis
14. Market Shares Analysis
15. Value Chain Analysis
16. Supply Chain Analysis
17. Strategic Analysis
18. Current & Future Market Landscape Analysis
19. Opportunity Analysis
20. Revenue and Volume Analysis

Frequently Asked Questions:

Q. Does IndustryARC publish country, or application based reports in Human Factor Security Market?
Response: Yes, we do have separate reports and database as mentioned below:

1. North America Human Factor Security Market (2018-2023)
2. South America Human Factor Security Market (2018-2023)
3. Europe Human Factor Security Market (2018-2023)
4. Asia Pacific Human Factor Security Market (2018-2023)
5. Middle East and Africa Human Factor Security Market (2018-2023)
6. Network Security Market in Human Factor Security Market (2018-2023)

7. Aviation Human Factor Security Market (2018-2023)

Q. Does IndustryARC provide customized reports and charge additionally for limited customization?
Response: Yes, we can customize the report by extracting data from our database of reports and annual subscription databases. We can provide the following free customization

1. Increase the level of data in application or end user industry.
2. Increase the number of countries in geography or product chapter.
3. Find out market shares for other smaller companies or companies which are of interest to you.
4. Company profiles can be requested based on your interest.
5. Patent analysis, pricing, product analysis, product benchmarking, value and supply chain analysis can be requested for a country or end use segment.

Any other custom requirements can be discussed with our team, drop an e-mail to sales@industryarc.com to discuss more about our consulting services.

To request for a proposal, provide your details in the below link:
https://industryarc.com/subscription.php

Media Contact:

Mr. Venkat Reddy
Sales Manager
Email: venkat@industryarc.com
Contact Sales: +1-614-588-8538 (Ext-101)

About IndustryARC:

IndustryARC is a Research and Consulting Firm that publishes more than 500 reports annually, in various industries such as Agriculture, Automotive, Automation & Instrumentation, Chemicals and Materials, Energy and Power, Electronics, Food & Beverages, Information Technology, Life sciences &Healthcare.

IndustryARC primarily focuses on Cutting Edge Technologies and Newer Applications in a Market. Our Custom Research Services are designed to provide insights on the constant flux in the global supply-demand gap of markets. Our strong team of analysts enables us to meet the client research needs at a rapid speed, with a variety of options for your business.

We look forward to support the client to be able to better address their customer needs, stay ahead in the market, become the top competitor and get real-time recommendations on business strategies and deals. Contact us to find out how we can help you today.

Venkat Reddy
IndustryARC
+1-614-588-8538
email us here
