Quantify risk and assess using the CMMI standard to reach right-sized maturity levels, goals and meet business objectives. Leverage a prioritized risk roadmap that generates insights to help identify clear levels of investments, budgets and resources to close critical gaps. Harness scalable efficiency in assessing capability maturity across the implemented controls that align with leading, globally respected frameworks like COBIT, ISO, NIST, CMMC and FFIEC.

ISACA's CMMI Cybermaturity Platform is a cloud-hosted assessment solution that leverages a risk-based approach to building enterprise cyber maturity and resilience. Enterprises that want to understand what maturity level is right for them, and how to get there, need the ability to:

1. Assess and manage risks effectively.
3. Improve alignment with enterprise strategy.
4. Enhance business resilience and security.

The Path to Mitigating Cybersecurity Risk is Building Cyber Maturity

Cybersecurity has become high stakes from Wall Street to the C-Suite. While enterprise leaders recognize that mature cybersecurity is essential to thriving in today's digital economy, they often lack the insights and data to have peace of mind that their organizations are efficiently and effectively managing cyber risk.

Managing Cybersecurity Risk: A Crisis of Confidence

At a time when cyberattacks have become the fastest-growing crime globally, confidence from board leaders in their organizations' preparedness is the exception, not the norm. This uncertainty is even more pronounced in a security landscape that has been further challenged by the COVID-19 pandemic.

Cybercrime damages are projected to cost the world US $6 trillion annually by 2021, up from $3 trillion in 2015.

Every 1.1 sec...

... But Confidence Is in Short Supply

COVID-19 Ups the Ante

Key Industries at Risk, Halting Business in its Tracks

<table>
<thead>
<tr>
<th>Industry</th>
<th>% of Small Companies</th>
<th>% of All Cybersecurity Breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare</td>
<td>41%</td>
<td>10%</td>
</tr>
<tr>
<td>Public/Government</td>
<td>53%</td>
<td>9%</td>
</tr>
<tr>
<td>Financial Services</td>
<td>58%</td>
<td>16%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>87%</td>
<td>20%</td>
</tr>
<tr>
<td>Technology</td>
<td>87%</td>
<td>20%</td>
</tr>
</tbody>
</table>

The healthcare industry also is subject to the highest volume of ransomware attacks. Financial and manufacturing services have the highest percent of exposed sensitive files. Supply chain cyberattacks were up 78% in 2019.

Businesses will fall victim to a ransomware attack in 2021.

The public/government sector is the target of 87% of all breaches.

The impact of COVID-19 on global cybersecurity risk.

The healthcare sector is the most targeted, accounting for 10% of all breaches.

SOURCES
- ISACA's CMMI Cybermaturity Platform provides an evidence-based approach to assess, grow, monitor and report on cyber maturity across the enterprise.
- For more information, visit www.cmmiinstitute.com/cybermaturity
- © 2020 ISACA. All rights reserved.