Cybersecurity by the Numbers

In the midst of COVID-19—in which 92 percent of IT audit and security professionals say cybercrime is increasing—data and information are critical, including data about cybersecurity performance: what does and does not work, how and where improvements can be made, and what peers are doing in their enterprises.

Increased Attacks, Rampant Underreporting and the Power of a Fully Staffed Team

Part 2 of ISACA’s global State of Cybersecurity Survey—a survey of more than 2,000 information security professionals from more than 17 industries—looks at threat landscape, the measures security professionals employ to keep their organizations safe, and key trends and themes in the practice of security.

Cyberattacks Are Still Increasing Year Over Year

Increased

Year Over Year

<table>
<thead>
<tr>
<th>Attack Methods</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social engineering</td>
<td>15%</td>
</tr>
<tr>
<td>Advanced persistent threat</td>
<td>10%</td>
</tr>
<tr>
<td>Ransomware and unpatched systems</td>
<td>9% each</td>
</tr>
</tbody>
</table>

ATTACKS ARE LIKELY—and So is Underreporting

Most Common Threat Actors

1. Cybercriminals 22%
2. Hackers 11%
3. Malicious insiders 10%
4. Nation-state attackers 9%
5. Hacktivists 8%

Fully Staffed Teams Are More Confident in Their Ability to Respond to Cyberthreats

Most Frequent Attack Methods

1. Social engineering (15%)
2. Advanced persistent threat (10%)
3. Ransomware and unpatched systems (9% each)

ATTACKS ARE LIKELY—and So is Underreporting

62% say they are underreporting in general

Hiring Time Matters

Who those who take longer to fill positions also report more attacks:

- 26% say it takes two weeks or less
- 35% say it takes three months
- 38% say it takes six months or more
- 42% say they cannot fill

Access full results at www.isaca.org/state-of-cybersecurity-2020 so you can assess how your enterprise’s efforts compare to other organizations and prepare for future attacks.

© 2020 ISACA. All rights reserved.