MIND THE GAP:

CYBERSECURITY’S BIG DISCONNECT

CYBERSECURITY RISKS ARE ESCALATING. SO WHY DO SO MANY ORGANIZATIONS CONTINUE TO MISS THE MARK IN DEFENDING AGAINST THEM?
Cybersecurity technologies and practices are constantly evolving to help organizations defend against persistent and increasingly malicious cyberthreats. But there’s more work to be done. Obvious disconnects have emerged between ever-shifting cybersecurity threats and organizations’ countermeasures.

According to the 2017 AT&T Global State of Cybersecurity survey, a cybersecurity attack has negatively affected nearly 80% of surveyed organizations in the past 12 months. The impact touches virtually every aspect of business.

Today’s leadership understands the variety of business risks from cyberattacks. What’s notable is the disconnect in how organizations are addressing these threats. Three areas of concern emerge from the AT&T survey:

- Overreliance on cyberinsurance
- Overconfidence in internal capabilities
- Underappreciation of cybersecurity awareness training.

Such critical gaps in current cybersecurity strategy could provide an open door to cybercriminals if left unchecked.

A Known Danger

Cybersecurity risks are escalating. Leaders now realize that cyberattacks continue to evolve, creating cybersecurity challenges that can threaten their business.

### Organizations’ top perceived threats in the year ahead

<table>
<thead>
<tr>
<th>Threat</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware, worms &amp; viruses</td>
<td>60%</td>
</tr>
<tr>
<td>Unauthorized access to corporate data</td>
<td>49%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>46%</td>
</tr>
<tr>
<td>Theft of proprietary company information</td>
<td>39%</td>
</tr>
<tr>
<td>Compromise of operational systems</td>
<td>38%</td>
</tr>
<tr>
<td>Compromise of mobile devices</td>
<td>35%</td>
</tr>
<tr>
<td>Advanced persistent threats (APTs)</td>
<td>33%</td>
</tr>
<tr>
<td>Identity theft of high-level corporate executives</td>
<td>32%</td>
</tr>
<tr>
<td>Compromise of IoT devices</td>
<td>32%</td>
</tr>
<tr>
<td>Denial of service</td>
<td>30%</td>
</tr>
<tr>
<td>Compromise of customer facing systems (e.g., PoS)</td>
<td>27%</td>
</tr>
<tr>
<td>Hijacking of social media accounts</td>
<td>24%</td>
</tr>
<tr>
<td>Website defacement</td>
<td>22%</td>
</tr>
<tr>
<td>Physical safety risks</td>
<td>21%</td>
</tr>
</tbody>
</table>

Ransomware is the #1 threat for those in the healthcare vertical (70%).

Source: AT&T 2017 Global State of Cybersecurity survey
Extended Impact
Cyberattacks can result in widespread impact across an organization. These impacts run the spectrum of business, from downtime to reputational damage to lost revenues and customers. Organizations can’t afford to ignore either the tangible or intangible damage resulting from a cyberbreach.

Mind the Gaps
While cybersecurity tools and defense techniques continue to advance, critical gaps in cybersecurity strategy can provide an open door to cybercriminals. In the AT&T survey, noticeable disconnects surfaced between evolving cyberthreats and organizations’ cybersecurity strategies.

How has a cybersecurity attack or successful breach affected your organization?

- Operational impact: 39%
- Downtime: 37%
- Damage to reputation: 25%
- Loss of revenue: 24%
- Loss of customers: 22%
- Loss of business partners/suppliers: 16%
- Regulatory fines: 15%
- Physical safety: 15%
- Legal consequences (lawsuits): 14%
- Diminished shareholder value: 11%
- Other: 1%
- None: 18%
- Don’t know: 1%

Source: AT&T 2017 Global State of Cybersecurity survey

28% of organizations see cyberinsurance as a substitute for cyberdefense investment.

65% say their in-house security capabilities are adequate, yet 80% were breached within the past year.

51% reported breaches from employee mobile devices over the past year, yet just 61% mandate awareness training for all employees.

Are You Keeping Pace?
Today’s leadership understands the variety of risks from cyberattacks. But conspicuous disconnects exist in how organizations are addressing these threats. To keep pace with the evolving threat landscape, consider a multilayered approach to cybersecurity.

The average cost of a data breach in 2017 was $3.6 million.

Source: Ponemon Institute