The State of Cyber (In)Security

Companies are nearly 3 months behind in detecting intrusions

<table>
<thead>
<tr>
<th>Year</th>
<th>Average time until detection (in days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>57.6</td>
</tr>
<tr>
<td>2016</td>
<td>80.6</td>
</tr>
<tr>
<td>2017</td>
<td>92.2</td>
</tr>
</tbody>
</table>

More devices, more problems

- 20,000,000,000 Internet-connected devices in use by 2020
- $6 TRILLION Estimated annual cost for cybercrime by 2021

Nearly all companies are impacted

In 2017, companies report being affected by:

- 36% phishing schemes
- 17% ransomware
- 9% email hacking

Companies that experienced losses due to cybercrimes

- 70% in 2017
- 64% in 2016

Nearly 1 in 5 businesses saw critical system interruption due to security events in 2017:

- Internal systems slowed
- Customer support offline
- Non-functioning products
- Website down

The common denominator in cyberattacks?
Social engineering, or the manipulation of users and employees.

and yet...

48% of companies have no formal procedures for responding to threats

The problem is bigger than you know, think or fear ...
Every endpoint is an entry point ... and there is no such thing as too much security.

Sources: Celent, CSO, Gartner, Herjavic Group, Pew Research Center

getinfo@fisglobal.com | fisglobal.com | 800.822.6758

©2017 Fiserv, Inc. All rights reserved. Fiserv and the Fiserv logo are registered trademarks of Fiserv, Inc.