3 Steps to Stop Employees From Taking Cyber Bait
How to turn employees into cybersecurity assets
Introduction

The volume of cyberattacks increased over 100% in Europe, East Asia and Latin America in October and November 2020. Canada and Germany each saw a 250% increase. The average ransomware payment in 4Q20 topped $150K. And it’s not just the volume of attacks that’s rising. Attacks are becoming more sophisticated and people are often the ones opening the door.

Cybercriminals have become experts at social engineering skills, tricking employees into clicking on malicious links that initiate attacks. While security and risk management leaders know that social engineering is a top risk, many still struggle to stop employees taking the bait. Remote work has only increased the risks — with employees facing confusing security policies while using more home networks and personal devices.

This guide addresses three common challenges to building a defensible security awareness program:

1. Initiatives to increase employee awareness are random or one-off, so employees complete awareness training tasks but don’t actually learn how to change their behavior.

2. Awareness is stuck in a compliance mindset that prioritizes check-the-box training over driving risk outcomes.

3. Leadership doesn’t see value in awareness, which results in a lack of resources and tepid support.

No security control is perfect — but effective controls help manage risk. Our practical advice helps turn employees into controls that detect and resist social engineering attacks.

William Candrick
Director Analyst, Gartner
Security & Risk Management

---

36% of data breaches involve phishing, up from 25% from the prior year.

85% of data breaches involved a human element.

Source: Verison 2021 Data Breach Investigations Report
Cyber risk is top-of-mind in boardrooms

Boardroom perception of top enterprise risks
Percentage of responding board directors

- Regulatory/Compliance Risk: 60%
- Cybersecurity: 48%
- Business Execution Risk: 43%
- Employee Related: 41%
- Finance Related: 33%
- Competition: 33%
- Economic Disruption: 29%
- Digital Disruption: 29%

n = 133
Q: What are the top sources of risk to the enterprise?
Source: 2020 Gartner Board of Directors Survey
Help employees stop ransomware

The initial entry point for a ransomware attack (ingress) often takes the form of a compromised website delivered through a phishing or targeted attack. Remote desktop protocol, bring-your-own-PC, and virtual private network vulnerabilities and misconfiguration are becoming the most common entry points for ransomware attackers. This has been exacerbated by the growth in remote work resulting from the pandemic.

- **$154,108**: Average ransomware payment in 4Q20
- **10x-21x**: Average downtime during attacks in 4Q20
- **70%**: Cases featuring threats to leak exfiltrated data in 4Q20

Source: Gartner, Coveware Quarterly Ransomware Report
Develop a defensible awareness program

Challenge
- Awareness efforts become ad hoc
- Awareness is stuck in a compliance mindset
- Leadership doesn’t see value in awareness

Solution
01 Develop a list of signature behaviors
02 Measure outcomes, not activities
03 Connect awareness to business benefits
# Develop a list of signature behaviors

Illustrative examples of signature behaviors in a vision statement (template below)

<table>
<thead>
<tr>
<th>Desired practices</th>
<th>Signature behaviors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Employees use strong passwords</td>
<td>We use passphrases to construct our passwords</td>
</tr>
<tr>
<td>2. Employees resist social engineering</td>
<td>We report suspicious emails to security</td>
</tr>
<tr>
<td>3. Employees protect sensitive information</td>
<td>We use secure, approved file transfer solutions</td>
</tr>
</tbody>
</table>
# Measure outcomes, not activities

Illustrative examples of activity and outcome metrics

<table>
<thead>
<tr>
<th>Activity metrics</th>
<th>Behavior outcomes metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of phishing simulations</td>
<td>Phishing simulation click rate</td>
</tr>
<tr>
<td>Number of training modules created</td>
<td>Average phish report rate</td>
</tr>
<tr>
<td>Number of newsletters published</td>
<td>Percent decrease in data loss prevention (DLP) alerts</td>
</tr>
</tbody>
</table>
## Connect awareness to business benefits

End-to-end example of how to link specific training and knowledge acquired to behavioral change, the desired operational outcomes to business outcomes and business benefits the organization’s senior executives actually care about.

<table>
<thead>
<tr>
<th>Security priorities</th>
<th>Business priorities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Awareness Training Activity</strong></td>
<td><strong>Knowledge Gained</strong></td>
</tr>
<tr>
<td>Phishing awareness training module</td>
<td>End users are better able to identify suspicious emails they receive</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Gartner

**SAMPLE METRICS**
- Percentage completion of mandatory training
- Number of cybersecurity incidents caused by phishing emails
- Reduced costs associated with incident remediation
- Reduced productivity loss associated with cybersecurity incidents
Actionable, objective insight

Explore these additional complimentary resources and tools for security and risk leaders:

- **Tool**
  - IT Score for Security and Risk Management
  - Understand how well your security function is performing in its current state and what improvements to prioritize.

- **Guide**
  - The IT Roadmap for Cybersecurity
  - Create a resilient, scalable and agile cybersecurity strategy.

- **Podcast**
  - Top Security and Risk Trends for 2021 Podcast
  - Emerging trends, expected challenges and next steps for security and risk management leaders.

- **Conference**
  - View Our Conference Calendar
  - Join a global community of CISOs and security and risk executives.

Already a client? Get access to even more resources in your client portal. **Log In**
Get More.

Get actionable, objective insights to deliver on your most critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

**U.S.:** 855 811 7593

**International:** +44 (0) 3330 607 044

Learn more about Gartner for IT Leaders
gartner.com/en/information-technology

Stay connected to the latest insights