



**GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY**
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Whitney, Lance

Title: “How to create a business-driven cybersecurity strategy: 3 tips”

Website: Techrepublic.com

Organization: TechRepublic

Date: 15 May 2019

URL: <https://www.techrepublic.com/article/lessons-your-business-can-learn-from-cybersecurity-trailblazers/>

Accessed: 15 October 2019

Synopsis: Cybersecurity is a necessity for any organization. But just adding more security professionals by itself isn't a sufficient strategy. Instead, a security team needs to support the company's strategic goals, argues PwC. In its latest Digital Trust Insights survey, the consulting firm has uncovered the so-called trailblazers, the top 25% of respondents who outperformed their peers at cybersecurity. The study released Wednesday reveals some of the lessons that can be learned from those companies identified as trailblazers.

Surveying more than 3,000 executives and IT professionals worldwide, PwC found one common thread among the trailblazers: Their security teams enhanced their mission from one of simply protecting business assets to one of being a strategic partner in the organization. As part of that approach, the security team is connected in an integral way to key executives responsible for devising corporate strategy, executing digital initiatives, managing risks, and monitoring the business.

How to create a business-driven cybersecurity strategy: 3 tips

Lance Whitney

Adding more security professionals isn't enough of a cyber strategy, according to new survey results from consulting firm PwC.

We're sorry, but a problem is preventing your video from playing.

Cybersecurity is a necessity for any organization. But just adding more security professionals by itself isn't a sufficient strategy. Instead, a security team needs to support the company's strategic goals, argues PwC. In its latest [Digital Trust Insights survey](#), the consulting firm has uncovered the so-called trailblazers, the top 25% of respondents who outperformed their peers at cybersecurity. The study released Wednesday reveals some of the lessons that can be learned from those companies identified as trailblazers.

Surveying more than 3,000 executives and IT professionals worldwide, PwC found one common thread among the trailblazers: Their security teams enhanced their mission from one of simply protecting business assets to one of being a strategic partner in the organization. As part of that approach, the security team is connected in an integral way to key executives responsible for devising corporate strategy, executing digital initiatives, managing risks, and monitoring the business.

SEE: [Special report: A winning strategy for cybersecurity \(free PDF\)](#) (TechRepublic)

More than 80% of the trailblazers surveyed said that their cybersecurity teams anticipated a new cyber risk to their digital initiatives, and managed it before it affected their partners or customers. Some 86% of the trailblazers saw their cybersecurity teams as adding significant value. And 58% of the trailblazers considered their security teams very effective as managing acute risks resulting from digital transformation.

The survey highlighted three ways in which cybersecurity teams at trailblazers are integrated into the business:

1. Connected on strategy

Cybersecurity teams are familiar with the business strategy. Among all the respondents, 65% of the trailblazers said they strongly agree that their cybersecurity team is embedded in the business, is conversant in the organization's business strategy, and has a cybersecurity strategy that supports business imperatives. That figure compares with just 15% of companies not identified as trailblazers who shared the same responses. As one example, this type of integration and support could mean that the cybersecurity professionals help design security into the company's products.

2. Connected on a risk-based approach

A full 89% of the trailblazers (versus 41% of others) said their cybersecurity teams are consistently involved in managing the risks inherent in the organization's business transformation or digital initiatives.

3. Coordinated in execution

Some 77% of the trailblazers (versus 22% of others) said their cybersecurity team interacts sufficiently with senior executives to understand the company's risk level related to core business practices.

For companies looking to shore up their cybersecurity efforts and strategy, PwC also offered insight based on the [US National Institute for Standards and Technology \(NIST\) Cybersecurity Framework](#). Specifically, the study uncovered how trailblazers fared at the framework's five core functions--Identify, Protect, Detect, Respond, and Recover.

Based on the survey, trailblazers have an edge over other companies at identifying assets and processes that need protection, but even they have room to improve, according to PwC. Few respondents reported high maturity at identifying physical and software assets at their companies for asset management.

Recovery planning was the most mature function among all respondents, but also the area where trailblazers showed the biggest lead. Businesses could improve their efforts at recovery planning through better communications and by incorporating lessons learned.

Trailblazers also showed an edge over other companies in the remaining three functions: Protect, Detect, and Respond.

For more, check out [How to create a transformational cybersecurity strategy: 3 paths](#) on TechRepublic.

