COMPUTERWORLD
FROM IDG
INSIDER EXCLUSIVE

What C-level leaders need to know about cybersecurity

Corporate boards are rarely prepared for cyberattacks and when they occur everybody likes to point fingers at everyone else

Stories in this package:

Corporate boards aren't prepared for cyberattacks

CEOs, board members need to bone up on cybersecurity and not leave those matters to CIOs, analyst says

Matt Hamblen / Computerworld

Major cyberattacks against organizations of all sizes seem to happen almost weekly. On Dec. 14, Yahoo announced the largest-ever data breach, involving more than 1 billion customer accounts.

Despite the scale and potential harm from such attacks, there's wide recognition that corporate leaders, especially boards of directors, aren't taking the necessary actions to defend their companies against such attacks. It's not just a problem of finding the right cyber-defense tools and services, but also one of management awareness and security acumen at the highest level, namely corporate boards.

"Our country and its businesses and government agencies of all sizes are under attack from a variety of aggressive adversaries and we are generally unprepared to manage and fend off these threats," said Gartner analyst Avivah Litan, a longtime cybersecurity consultant to many organizations.

"Some organizations do a better job than others, but those efforts are almost always led by CIOs, CISOs or business line managers and *not* by corporate boards, CEOs and executive management throughout government and the private sector," Litan added.

Litan said what's needed is a national response and cyber protection plan, but said she fears that the federal government is "way too fragmented and politicized to make any real progress toward this goal."

Threats against nationwide infrastructure, including the electricity grid, are "enormously serious," she added. "Unless senior executives, corporate boards and other senior stakeholders get their act together, the threat actors will continue to win. I'm not sure how many more wake-up calls we need in this country."

Litan's worries seem to have reached some quarters of the corporate governance community. The National Association of Corporate Directors (NACD) recently released a survey of more than 600 corporate board directors and professionals that found only 19% believe their boards have a high level of understanding of cybersecurity risks. That's an improvement from 11% in a similar poll conducted a year earlier.

The survey also found that 59% of respondents find it challenging to oversee cyber risk. The nonprofit NACD, which has 17,000 members, is working with security awareness firm Ridge Global and Carnegie Mellon University to create a Cyber-Risk Oversight program to educate corporate directors about the systemic risks of cyberattacks.

Litan said such education is important, but she also supports state and federal laws to require organizations to report cyber attacks so that customers and partners will know to change passwords and make other adjustments to protect sensitive data.

"Having a requirement to disclose is a great motivator to increase security to prevent future attacks," Litan said. "No one wants their names in the news. That's what corporate directors are most worried about, in fact."

A majority of states have data security breach notification laws, but so far there's no nationwide provision. California first enacted its notification law in 2003, and other states followed suit.

At the federal level, a number of U.S. senators have backed breach notification laws, but no bills have passed congressional muster. President Barack Obama proposed such legislation in 2015. With the January inauguration of Donald Trump as the next U.S. president, it remains to be seen whether a federal breach notification law will take effect in the next four years, or longer.

When Yahoo disclosed in September a separate hack dating back to 2014, U.S. Sen. Mark Warner, D-Va., renewed calls for bipartisan legislation to create a uniform data breach notification standard and co-founded the bipartisan Senate Cybersecurity Caucus. "Action from Congress to create a uniform data breach notification standard ... is long overdue," Warner said at the time.

One analyst, Jack Gold of J. Gold Associates, questioned whether a national breach notification law would be effective. "There are disclosure laws in many states and there are some government regulations that require disclosure, but I'm not sure it has any effect if companies lie about a hack or don't disclose it," he said.

IT and C-level leaders point fingers at each other over cyber defense

IT managers say a cyber attack will cost double what their bosses estimate, new poll finds

Matt Hamblen / Computerworld

IT managers disagree with chief executives over who is responsible for a cyber security breach, according to a survey released Thursday.

The survey -- of a group of 221 chief executive officers and other C-level executives and another group of 984 IT decision makers -- found that each group largely believes the other group is responsible in the event of a breach.

In the survey, 35% of C-level respondents said IT teams would be responsible in a breach, while 50% of IT leaders think that responsibility rests with their senior managers.

Also, IT managers estimate a single cyber attack will cost their business nearly twice what top-level executives estimate. The IT managers put the cost of a single attack at $19 million, compared to the C-suite estimate of about $11 million.

Opinium, an analyst firm, conducted the survey last October and November on behalf of BAE Systems Applied Intelligence, a cyber security and defense company.

The survey was conducted in the U.S. and seven other countries.

Overall, the results show "an interesting disparity between the views of C-level respondents and those of IT decision makers," said Kevin Taylor, managing director at BAE. "Each group's understanding of the nature of cyber threats, and of the way they translate into business and technological risks, can be very different."

He called for both groups to "bridge the intelligence gap to build a robust defense" against cyber attacks.

The survey lends support to the opinions of other analysts who say C-level executives need to get more informed on cybersecurity threats.

Tom Ridge, former secretary of Homeland Security, recently urged CEOs and corporate board to increase their level of cyber-risk awareness.

"Cybersecurity is the most significant governance challenge for the public and private sector," Ridge said in a recent interview. "It's not just the exclusive domain of the CIO and CTO, and is now in the domain of the CEO and the corporate board."

Ridge is currently the chairman of Ridge Global, a Washington-based cyber protection advisory firm.

The National Association of Corporate Directors surveyed more than 600 board directors and professionals last year, and found that only 19% believe their boards have a high level of understanding of cybersecurity risks.