abacode™
Cybersecurity Experts

# Cybersecurity Readiness Confidence Decline

## White Paper

April 7, 2017

# Summary

Tenable Network Security recently released the annual Global Cybersecurity Assurance Report Card for 2017, and the results are troubling. The global score, a 70 percent, shows a six-point drop from the 2016 report. This means that around the world, cybersecurity professionals are not confident in their abilities to prevent cyber-attacks, because the hackers are several steps ahead.

Though the score drop was chiefly due to new technologies developing too quickly for security professionals to keep up, the issue must be remedied. The most efficient way to reduce instances of cyber-crime is through training and awareness, especially of employees.

# The Issue

Last year, the first year Tenable Network Security released the Global Cybersecurity Assurance Report Card, the global score was a 76 percent. The United States had an 80, and now stands at 78 percent when it comes to confidence when dealing with cybersecurity issues. In fact, nearly every country examined both years experienced a drop in their scores, with the exception on Australia.

The reason for this decline? Risk assessment, which dropped an average of 12 percent worldwide compared to last year's report. Risk assessment is key, so this is extremely significant seeing as cybersecurity experts around the world do not even know what the dangers are because new devices, networks, and technologies are appearing at an alarming rate. Hackers are evolving with them, leaving cybersecurity experts at a loss as to where to begin in terms of prevention and defense.

Which industries took the largest hit this year in terms of preparedness? Tenable Network Security found that the Financial Services, Telecom and the Health Care Industry scores suffered the most compared to last year's report, but every industry studied underwent a score drop. The health care industry in particular has always been vulnerable to breaches, and with the surge in ransomware incidents at hospitals this year, health care is certainly a top priority when it comes to cybersecurity enhancements.

# The Reason

In short, technology is developing faster than cybersecurity experts can keep up. Cyber criminals, on the other hand, continue finding more pathways into various new devices and networks and more creative ways to hack into older technology. The exponential growth of technology along with hacker abilities keeps security professionals guessing as to which risks

are being taken advantage of at what times, especially since cybersecurity framework must guard many ways in, while hackers only need to find an exploit a single one.

Rising technology, particularly mobile devices, containerization (the use of multiple systems being launched and run for multiple apps) and DevOps (the collaboration of IT professionals and software developers), ultimately caused the failing average grade received by countries and professionals when it came to risk assessment by security experts. The risk assessment suffers with these emerging technologies because the decentralization accompanying them means that professionals cannot detect everything on their networks at all times.

A constantly evolving threat environment is good news for cyber criminals, as it gives them more opportunities to manipulate every day, and bad news for everyone else, as everyone is at risk now. The threat environment has been the number one challenge faced by cybersecurity teams two years in a row, and it is time to take action. No matter how much time or money is spent on cybersecurity by a business, if they do not take realistic measures to assess their preparedness in the case of a security compromise, they are likely to be attacked. Everyone is a target.

## The Solution

The bottom line? Training is crucial. Particularly in businesses, employee training is essential for preventing cyber-attacks. Individuals must be aware of the risks they face, the methods hackers can use to manipulate them and penetrate networks, and the damage that can be wreaked on a business or a person's life as a result of cybercrime.

Abacode not only provides a training program to ensure that employees know how to protect themselves and keep the organization from being vulnerable. We will also perform a technical discovery to uncover weaknesses in company databases and monitor networks and data to learn about and prevent breaches in real time.

Monitoring is certainly the most important step in protecting company and personal data, but humans have always been the weakest link in the chain of defenses against cyber-crime. Training minimizes the risk of human error so that small mistakes do not lead to larger issue such as falling prey to social engineering or the novel and harrowing ransomware gaining popularity.

Abacode provides every necessary element to reducing personal and company risks of cyber-attacks. Though worldwide, the standards of cybersecurity are lacking, the problem can be remedied before it does even more damage, so long as awareness is increased and the correct actions are taken.