Cyber security is ambiguous. So ethereal in fact, that many don't understand the complexities of how it works and what's involved in protecting an organization. This lack of knowledge perpetuates ideas about the field that just aren't true—and it's hurting businesses that are working hard to boost. Today, we're debunking some of the most common cybersecurity myths, so we can help organizations find effective solutions that protect them.

A strong password, regularly updated, is not enough to keep business or personal accounts safe from hackers. Two-factor authentication and data monitoring are also needed. Although two-factor authentication adds an extra layer of security, it can still be bypassed through phishing attacks and Man In The Middle (MITM) attacks.

Not all cyber threats come from sources outside of an organization. Inadvertent threats can also come from users, employees, and external contractors within your organization who have authorized access to a network. In the United States alone, more than 2,500 Internal Security Breaches occur every day.

Cyber security training and readiness solutions can seem too expensive to achieve, but they don't have to be. An investment in cyber security preparedness is nominal compared to the damaging outcomes of brand deterioration and the loss of revenue, sensitive data, and constituent trust. The global average cost of a data breach exceeds $3.8 million—far more than an investment in a cyber training solution.

True complete protection from cyber threats can never fully be achieved. Just as technology and security methods advance, so do the approaches of hackers who are constantly looking for new ways to exploit vulnerabilities. Cybersecurity is an ongoing endeavor, one that shouldn't rest on the laurels of periodically trained staff. Organizations need a persistent training solution equipped with an evolving library of threat scenarios available on a virtual cyber range that emulates company networks.

Learn how Project Ares training and assessment solutions can strengthen your cybersecurity readiness.

It is not always apparent when a cyber attack has occurred and sometimes intruders can linger for long periods of time without detection. Modern malware and nation state organizations are getting creative and stealthy about how they enter and exploit a system.

Cyber security is not just an IT department issue because hackers can target all levels of the company from contractors to the CEO. Experts are calling on CISOs to have a more visible seat at the c-suite table to align security strategies with company objectives.

All industries are susceptible to a cyber attack regardless of the sensitivity of the data they carry. Sometimes hackers will target less sensitive data in order to build up to a larger attack. For example, nation state hackers are often out to undermine trust in critical services and manipulate public attitudes (e.g. as seen in election hacking).

Hackers are equally as interested in small businesses as they are large corporations. Every company, should be investing in cyber defense and training for employees. Across the United States, nearly 57% of small businesses have seen an increase in cyber attacks.

Although it is still important to have the latest software installed, frequently updating software and systems alone will not prevent a cyber attack. To protect the entirety of an organization, comprehensive cyber solutions are needed to address multiple fronts: from employee training, to threat detection, to incident response, to forensic investigation.

Traditional cyber training classes alone will not bring your team up to speed and prepare them for evolving cyber threats. These classes employ passive-learning techniques like slide decks and videos to present information, much of which is outdated and forgotten by the learner after the first month. These techniques yield a 5% information retention rate whereas active-learning approaches increase retention rates to 75%.

© 2019 Circadence Corporation

The Circadence logo, Project Ares, and the Project Ares logo are trademarks or registered trademarks of Circadence.

1 https://www.securitymagazine.com/articles/89586-nearly-70-percent-of-smbs-experience-cyber-attacks
5 https://cdns3.trainingindustry.com/media/3203537/game%20based%20learning.pdf