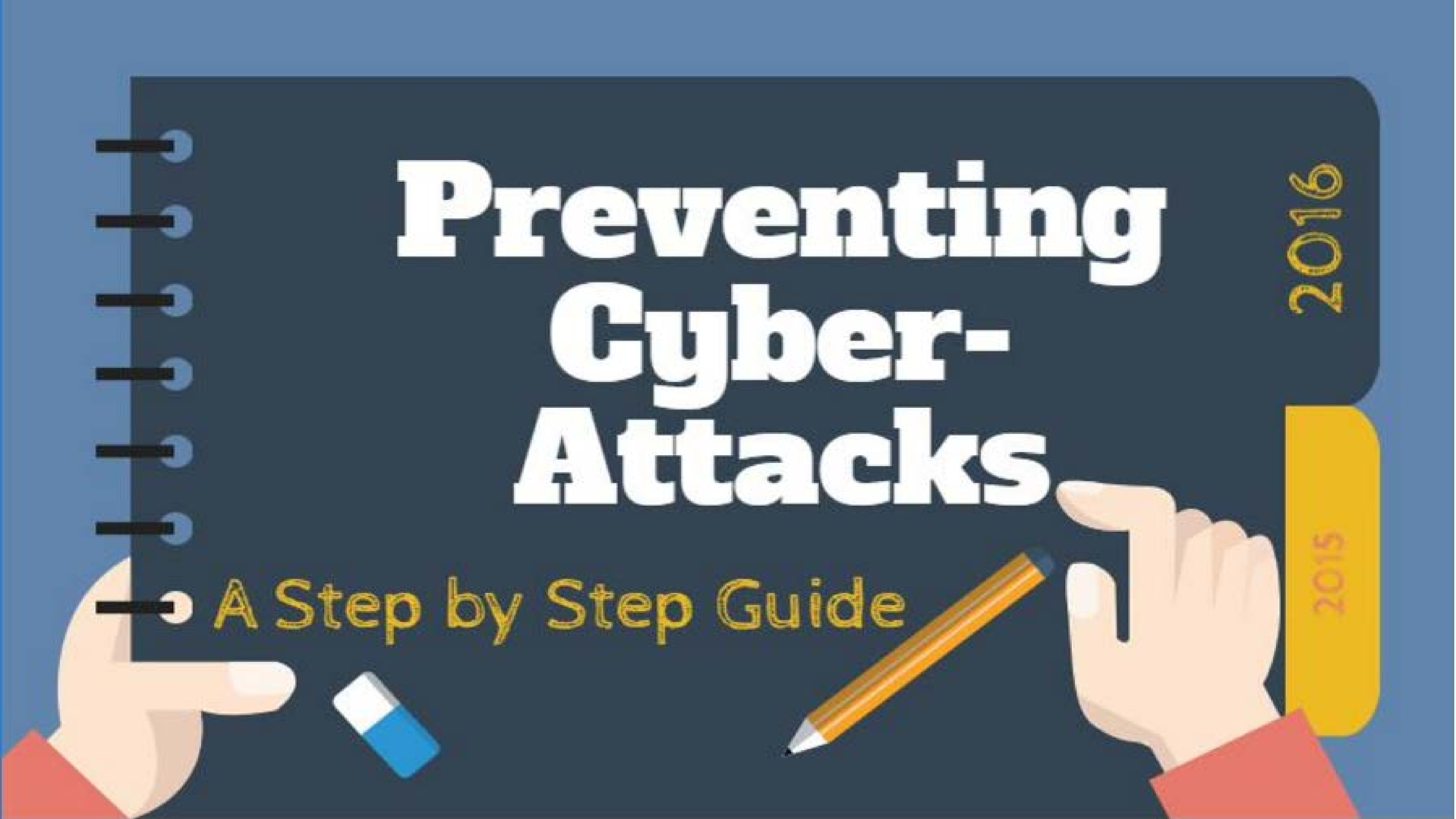

Preventing Cyber-Attacks

A Step by Step Guide

Step 1:
THEY FIND THE WEAKEST LINK

Stolen user credentials are still the #1 way hackers get into your system. Keep employees vigilant with education and testing, especially with regards to phishing emails which 23% of employees are still opening and 11% are clicking on.

Step 2:
THEY BREACH THE PERIMETER

In 60% of cases, attackers are able to compromise an organization within minutes, and 99% of exploited vulnerabilities were compromised more than a year after the CVE was published. Focus on prioritizing risk, not on fire drills updating patches each time they are released.

Step 3:
THEY USE YOUR VPN

While companies spend up to 85% of their budgets protecting their perimeters, attacks can still happen through using stolen user credentials and coming in through the VPN. Make sure your IAM solution monitors for unusual access behavior.

Step 4:
THEY PLAY HIDE & SEEK

75% of attacks spread from Victim 0 to Victim 1 within 24 hours. Keep hackers from working their way through your network by continuously and comprehensively monitoring all access with an intelligent IAM solution.

Step 5:
THEY STEAL YOUR DATA

Hackers like to download malware into your network malware into your network to be able to exfiltrate data. Malware events occur every five seconds and most are unique to your organization. Without vulnerability and access management, you could miss not only the attacker getting in but the information getting out.

TIRED OF BEING ON DEFENSE?

With Core Security you can be proactive, not reactive, about your cybersecurity. From continuous and comprehensive monitoring of your vulnerability and access risk systems to attack path modeling, we can help you go on offense.

Contact us today for a trial, demo, or to hear more about how our solutions can work for you.

info@coresecurity.com

www.coresecurity.com/blog