Incidents & Innovations in Government Cyber Security Training

CIRCADENCE

Government agencies and organizations are prime targets for cyberattacks

Whether a state, local or municipal entity, many organizations aren't equipped with the proper resources to defend and protect their networks—and constituents. From records on critical infrastructure, to citizen payment information, to social security numbers and addresses, attackers know there is a treasure trove of data ready to be stolen if the right hacks are deployed on vulnerable systems.

In the middle of 2019 alone, government agencies have experienced a slew of attacks aimed to compromise the target's security efforts and ensue political unrest. The timeline snapshot below illustrates the frequency and unfortunate reality of cyberattacks in the government sector, with incidents reported by the Center for Strategic International Studies.

May 2019
Government organizations in two different Middle Eastern countries were targeted by Chinese state-sponsored hackers.

June 2019
Chinese intelligence services hacked into the Australian University to collect data they could use to groom students as informants before they were hired into the civil service.

July 2019
Croatian government agencies were targeted in a series of attacks by unidentified state sponsored hackers.

It's very likely that there are many more attacks on the government sector than are ever reported. Some governments may also be entirely unaware that there is malware already installed on some of their systems and the attackers are just waiting for a politically beneficial time to activate their attack.

July 2019
A Chinese hacking group was discovered to have targeted government agencies across East Asia involved in information technology, foreign affairs, and economic development.

August 2019
Networks at several Bahraini government agencies and critical infrastructure providers were infiltrated by hackers linked to Iran.

August 2019
The Czech Republic announced that the country's Foreign Ministry had been the victim of a cyberattack by an unspecified foreign state.

(Source)

Ransomware

The most high-profile municipal ransomware attack took place over a year ago in March 2018 when the city of Atlanta was crippled by SamSam ransomware. According to Wired magazine, the city of Atlanta ended up spending $2.6 million to respond to that attack, roughly 52 times the amount of the $50,000 or so in ransom demanded by the attackers.

Malware

Threat group Cloud Atlas has conducted severe cyber espionage operations on multiple government, diplomatic, and research organizations using a new piece of polymorphic malware called PowerShower. The malware is designed by procure PowerShell and VBS modules that can be executed on a compromised machine, reports SecurityWeek. This malware allows attackers to steal documents and passwords from devices.

DDoS Attacks

In April 2007 the nation of Estonia was hit with a massive DDoS attack targeted at government services as well as financial institutions and media outlets. This had a crushing effect since Estonia's government was an early adopter of online government and was practically paperless at the time; even national elections were conducted online, reports CloudFlare.

Cyber Espionage

Cyber espionage is an act of gaining unauthorized network or system access, usually to obtain the sensitive data of a government or a military infrastructure using proxy servers. Hacking group APT39 in Iran is one of many groups considered a critical threat to U.S. national security, alongside Russia and North Korea. In addition, United Arab Emirates used the spying tool Karma to hack the iPhones of activists, diplomats and rival foreign leaders, reports Reuters.

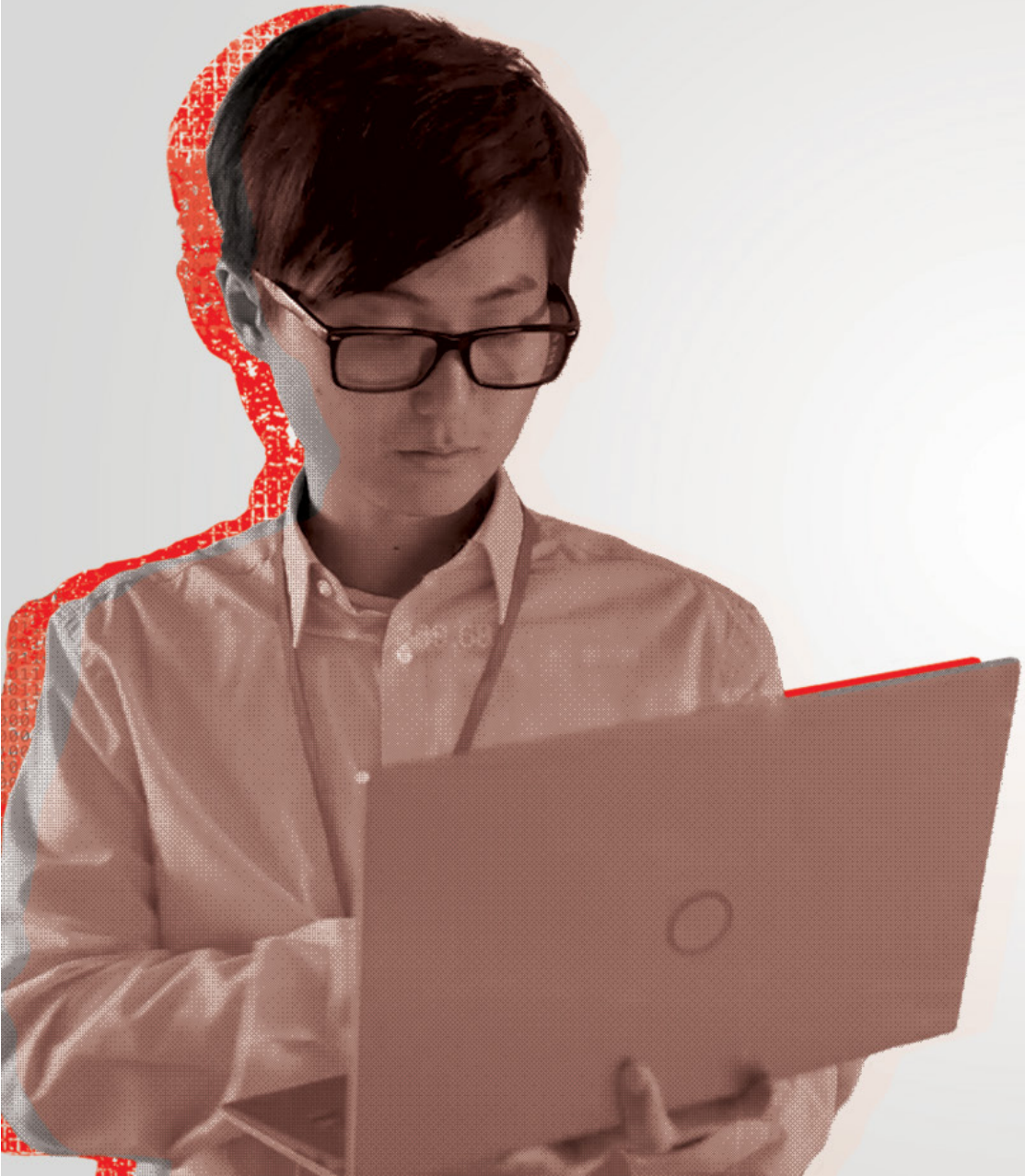
"Most people don't realize cities have massive amounts of data. It's amazing the different types of data that they have. I mean it's just phenomenal. They have everything from permits to people paying their water bills to parking tickets to whatever. U.S. cities are very, very similar to large multinational businesses."

Gary Hayslip

Former CISO for the City of San Diego, California

Innovations in Cyber Security for Government Entities

Governments at all levels are taking steps to leverage advancements in technology and security to proactively protect its people, data, and reputation. Today's innovations offer ground cyber learning in **real-world, practical experiences and examples** so people of all competency-levels can understand the impact a simple link click or opened email has on the security of a government organization.



Upskill the Cyber Workforce

Hyperscalable cyber training has been a renewed focus for governments looking for ways to upskill their cyber teams with relevant and “sticky” learning opportunities. Cloud-based cyber ranges that provide training exercises for individual and team-based collaboration are proving effective in preparing cyber professionals to hone their competencies.

PROJECT®
ARES

Project Ares® gamified cyber learning platform running on Microsoft Azure, helps teams enhance their security knowledge and application in real-world settings. Artificial intelligence and machine learning features automate and augment routine cyber security tasks for trainees so they can dedicate more energy toward building skills reflective of agency-wide cyber strategy.

Platforms like Project Ares give CISOs and security directors visibility into the weaknesses of their team and help them identify cyber learning paths for teams to pursue.

Summing it up

Partisanship is political. Cyber is not. While federal, state and local governments can't prevent more cyberattacks from occurring, security leaders can learn from the past and use learned lessons to inform their adoption of new innovations in the market today.

Further implementation of advanced training and cyber learning resources like the ones offered by Circadence will aid to increase cyber security protection of critical government networks and systems worldwide.

CIRCADENCE

Circadence® Corporation is a market leader in cyber security learning, offering gamification as a tool to create engaging, immersive learning that sticks and a product portfolio that address cyber learning needs from security awareness to complex cyber team interaction.

Schedule a demonstration of Project Ares:
https://www.circadence.com/request-a-demo/

Microsoft Gold Partner

SC 2019 awards Winner

INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2019

Info Security Products Guide 2019 GLOBAL EXCELLENCE GOLD

CYBER SECURITY EXCELLENCE AWARDS WINNER 2019