ADDRESSING THE EVOLVING CYBERTHREAT LANDSCAPE

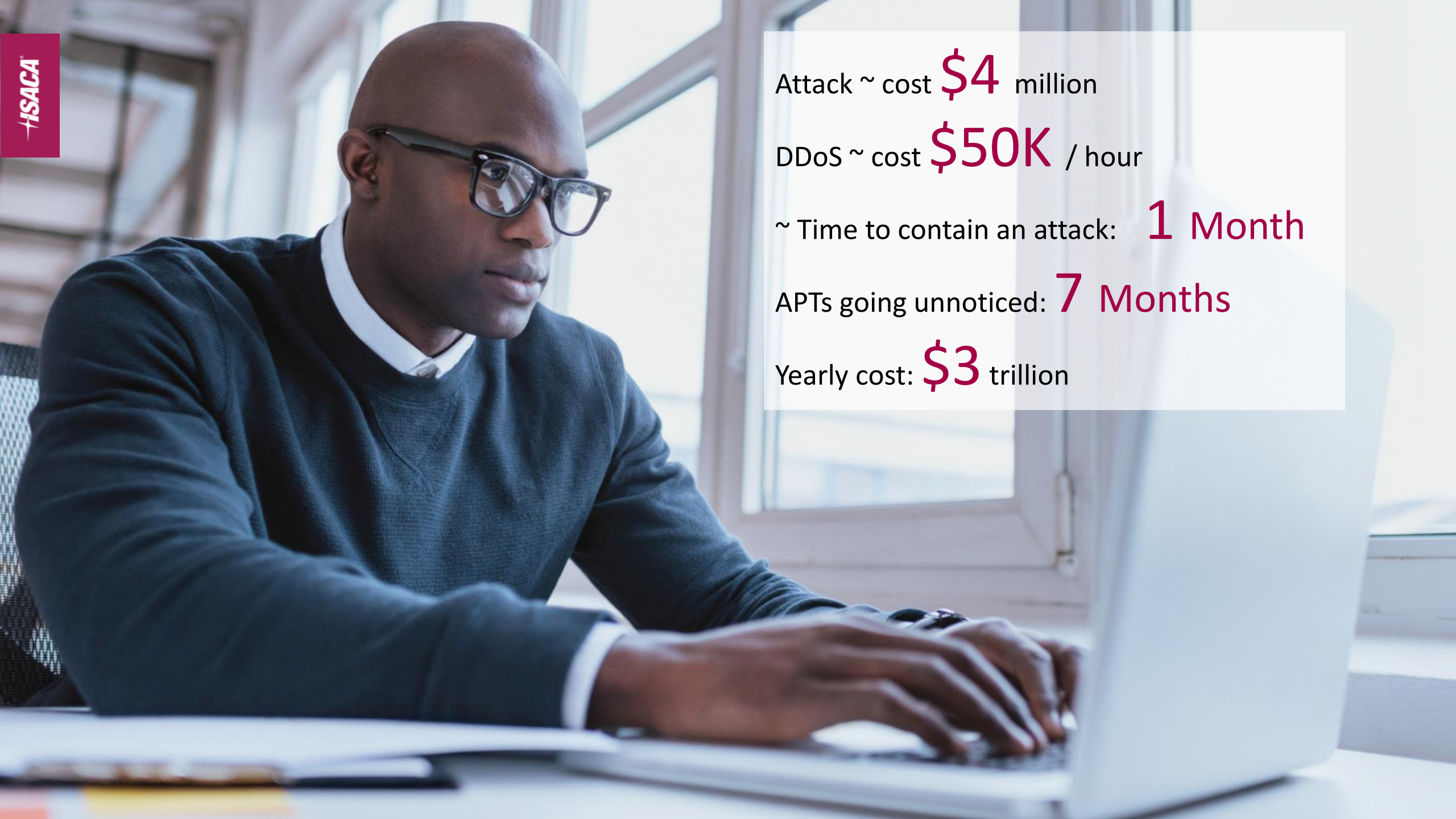
Dr. Christos K. Dimitriadis, CISM, CISA, CRISC
Chair, ISACA Board of Directors
Group Director of Information Security, INTRALOT

Agenda

1. Cyber Threat Landscape 2016
2. Building Cyber Security Capability

Global environment

- Technology proliferation = “The 4th Industrial Revolution”
  World Economic Forum Summit on the Global Agenda
- Fortune 500 life expectancy: 1975=55y, 2016=10y
- IoT: 2009 / 2,5b devices, 2020 / 30b devices (GARTNER)
- By 2018 owned infrastructure will be <50%
  the rest is Cloud (Forrester)
- Software: From Monolithic->SoA-> Microservices


ISACA
Attack ~ cost $4 million
DDoS ~ cost $50K / hour
~ Time to contain an attack: 1 Month
APTs going unnoticed: 7 Months
Yearly cost: $3 trillion

Cyber Threats

- U.S. Department of Homeland Security: **60%** of Cyber Attacks originate in supply chain
- Verizon 2016: **80%** of breaches occurred from externals
- Main Motives: financial / espionage
- EY Global Data Analytics 2016: Fraud main tools are cyber breaches combined with internals – bribery/corruption follows

ISACA State of Cyber 2016: Cyber threats

- **82%** report their Board of Directors are more concerned
- **Only 20%** of CISOs report to the CEO/Board
- **45%** hiring increase in 2016
- **94%** report difficulty in finding skilled professionals
- **31%** of attackers were criminals
- **24%** are still unknown
- **Most successful attacks:** Phishing, malware, social engineering

ISACA 2016 Cyber Security Jobs Index

- **781** data breaches reported in 2015…in the US alone (second highest year on record)
- **About 75%** of attacks focused on the business or health/medical industries
- **27%** of cyber security positions are requiring up to 6 months to fill
- **59%** of security professionals say that less than half of the job candidates they considered were “qualified upon hire”—an increase of nearly 10% from the prior year

Building Cyber Security Capability *(Based on US-NIST / CSX)*

IDENTIFY

- Business Impact Analysis / Assets Discovery / Prioritization
- Risk management as part of ERM
- Policies, Procedures
- Organization
- People

Building Cyber Security Capability *(Based on US-NIST / CSX)*

PROTECT

- Technology (Infrastructure, Network, DB, OS, Application)
- Data Security policies, processes, controls
- People (Training and Awareness)
- 3rd Parties / Supply Chain

Building Cyber Security Capability *(Based on US-NIST / CSX)*

DETECT

- Technology
  - Logging
  - Monitoring
  - Correlation
  - Anomaly Detection
- Detection Processes
- Detection Teams, Roles, Responsibilities
- 3rd Parties

Building Cyber Security Capability *(Based on US-NIST / CSX)*

RESPOND

- Response Teams, Roles, Responsibilities
- Incident Management Procedure / Response Plans
- Analysis process, Mitigation
- 3rd Parties / Authorities / Experts
- Testing and Improvement
- Communications / PR
- Information Sharing

Building Cyber Security Capability *(Based on US-NIST / CSX)*

RECOVER

- Recovery Teams, Roles, Responsibilities
- Restoration Planning / Business Continuity
- Data recovery
- Cyber Insurance
- Communications / PR
- Testing and Improvement

Holistic Cyber Security Program

- CSX is designed to help fortify and advance the industry by educating and training a stronger, more informed workforce that can keep organizations and their information secure—now and in the future. CSX provides expertise and insights, guidance, training and educational events to meet the needs of individual professionals and organizations.

Cyber Security Fundamentals

CSX CYBERSECURITY™
FUNDAMENTALS CERTIFICATE

- The entry point into ISACA's cyber security program, Cyber Security Fundamentals, offers a certificate in the introductory concepts that frame and define the standards, guidelines and practices of the industry. The certificate and related training are ideal for college/university students and recent graduates, those new to the field, as well as those looking to change careers.
- The Cyber Security Fundamentals exam tests for foundational knowledge across five key areas:
  - Cyber security concepts.
  - Cyber security architecture principles.
  - Cyber security of networks, systems, applications and data.
  - The security implications of the adoption of emerging technologies.
  - Incident response
- The exam is available online, and may be taken at home or in office.
- Multiple options are available to help prepare for the Cyber Security Fundamentals Certificate exam: the accompanying study guide, an 8-hour online course, and 2- or 4-day workshops available during ISACA events

CSX Website

- The CSX site is the main hub for ISACA's holistic cyber security program. Explore all that CSX has to offer at https://www.cybersecurity.isaca

Additional Reading

ISACA CSX (CyberSecurity NEXUS) http://www.isaca.org/cyber/

US NIST Cybersecurity Framework https://www.nist.gov/cyberframework

THANK YOU

cdimitriadis@isaca.org

@DimitriadisC

@ISACANEWS