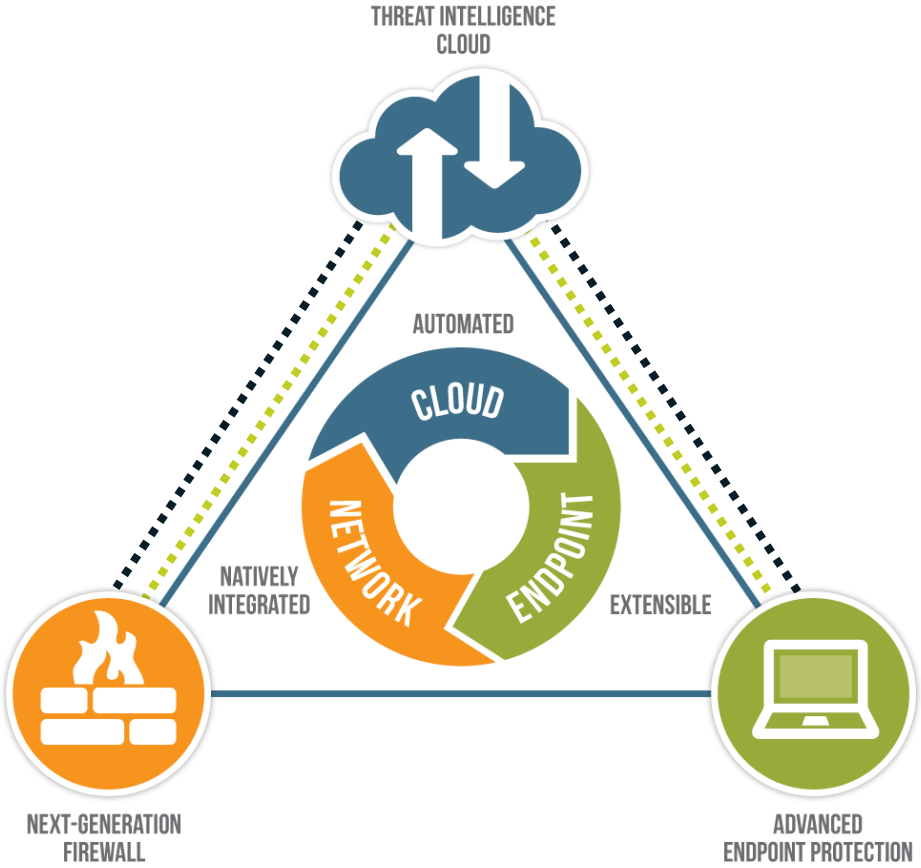
Cybersecurity, Trade, and Economic Development

G7 ICT Priorities: Technology, Innovation, and the Global Economy
UNCTAD E-Commerce Week

Danielle Kriz
Senior Director, Global Policy
Palo Alto Networks

April 18, 2016

Delivering the next-generation security platform

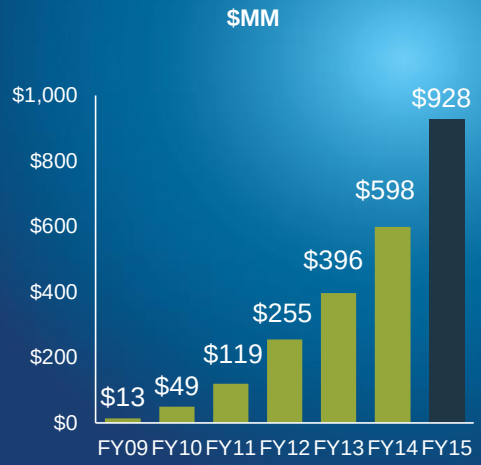


Palo Alto Networks at-a-glance

CORPORATE HIGHLIGHTS

- Founded in 2005; first customer shipment in 2007
- Safely enabling applications and preventing cyber threats
- Able to address all enterprise cybersecurity needs
- Exceptional ability to support global customers
- Experienced team of 3,300+ employees
- Q2 FY16: $334.7M revenue

REVENUES



ENTERPRISE CUSTOMERS

G7 Recommendation- Cybersecurity

"The G7 can demonstrate global leadership on ICT priorities if it agrees on the following outcomes in 2016:

Cybersecurity. Ensuring that measures they take to enhance cybersecurity **reflect the global nature of cyberspace**, **rely on risk management-based approaches** that avoid prescribed standards for individual technologies, and **incorporate meaningful consultation with the private sector** to encourage innovative, flexible, and cost-effective solutions."

Why is this approach important?

Cybersecurity measures should …

…reflect the global nature of cyberspace

- **Cyberspace is global**
  - **Global Internet – technologies must interconnect**
  - **Companies need to work online across borders**
  - **People need to communicate across borders (using an iPhone in Switzerland to call a friend on an Android phone in Mozambique)**
- **Threats are global**
  - **Cyber criminals do not respect national borders**
  - **Threats cross borders in real time**
  - **Countries (their businesses and citizens) face many of the same threats**
- **Security measures must also be global**

Cybersecurity measures should …

…rely on risk management-based approaches

- **Organizations often have different risks from each other**
  - **Can depend on their industry, location, sophistication, size, and assets**
  - **They may have different things of value that criminals want**
  - **They could be targeted for other reasons (e.g. political reasons)**
  - **They use various technologies, infrastructure, applications**
- **And these risks change over time**
  - **Items of value change**
  - **Companies enter new lines of business, get new customers or partners**
  - **Cyber criminals change tactics**
  - **Technologies change**

Cybersecurity measures should …

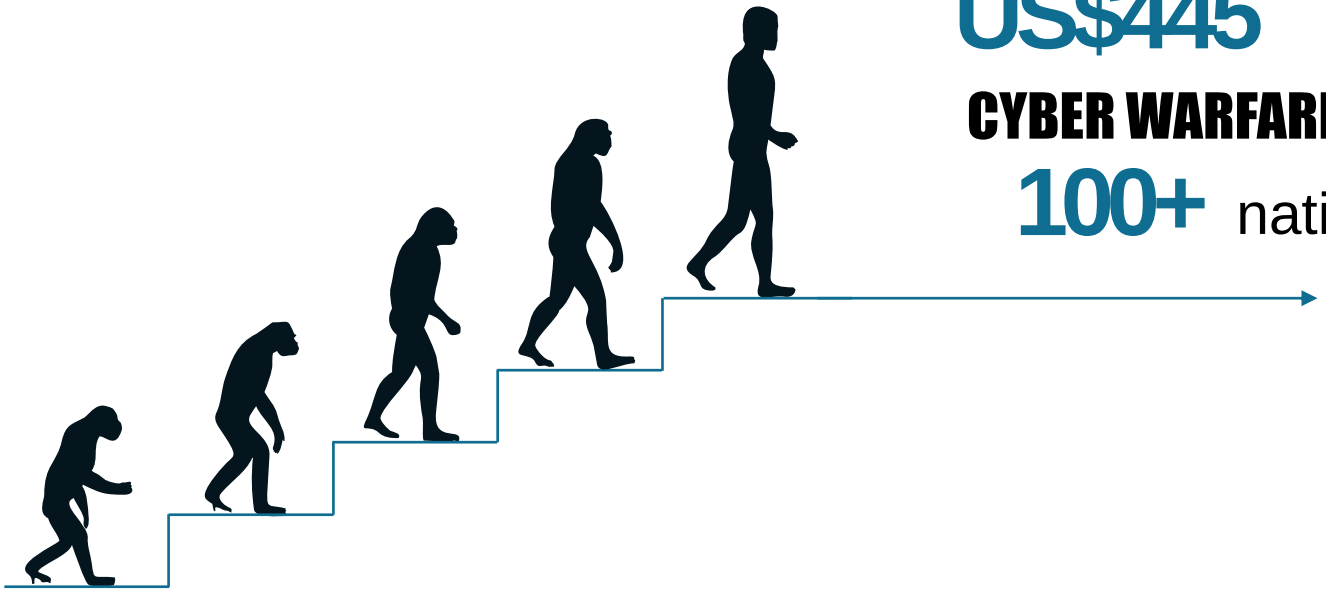
…incorporate meaningful consultation with the private sector

- **Expertise exists everywhere**
  - **Knowledge about threats, technologies- much of this is in private industry**
- **Governments and the private sector have the same goal: better cybersecurity and resilience**
  - **Governments want to protect their citizens, businesses, and economies**
  - **Companies want to conduct business securely, protect their IP, and protect their customers' data**
  - **In many countries, private companies own or operate critical infrastructure**
- **Companies have significant experience with cybersecurity**

CYBERSECURITY IS A COMPLEX POLICY ISSUE

What's changed?

THE EVOLUTION OF THE **ATTACKER**



CYBERCRIME NOW

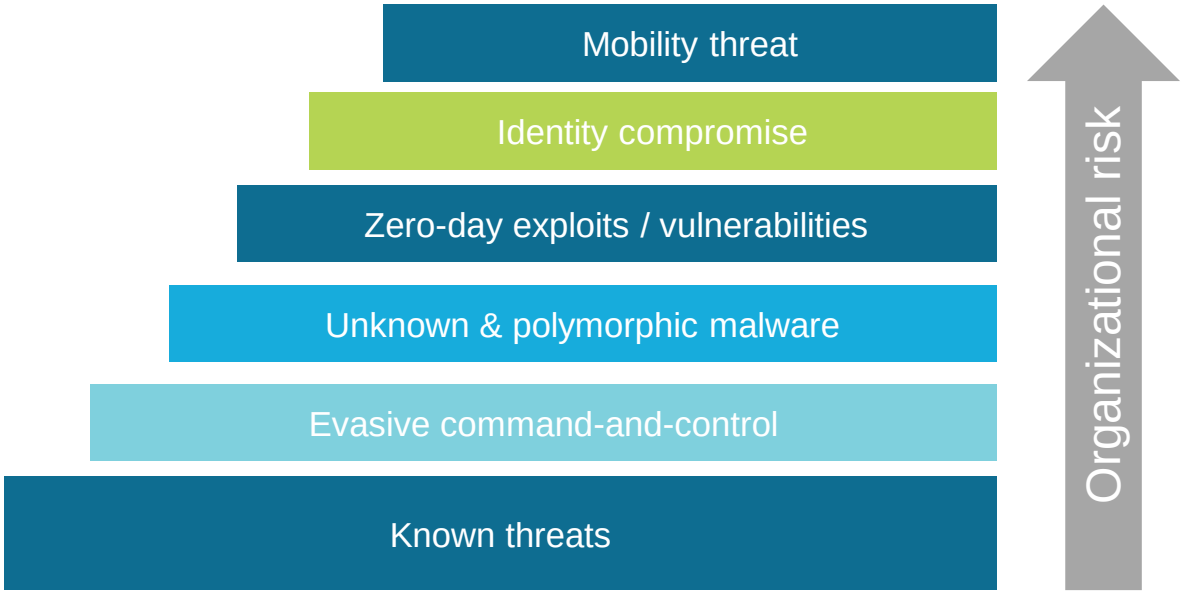
US$445 billion industry

CYBER WARFARE

100+ nations

What's changed?

THE EVOLUTION OF THE **ATTACK**

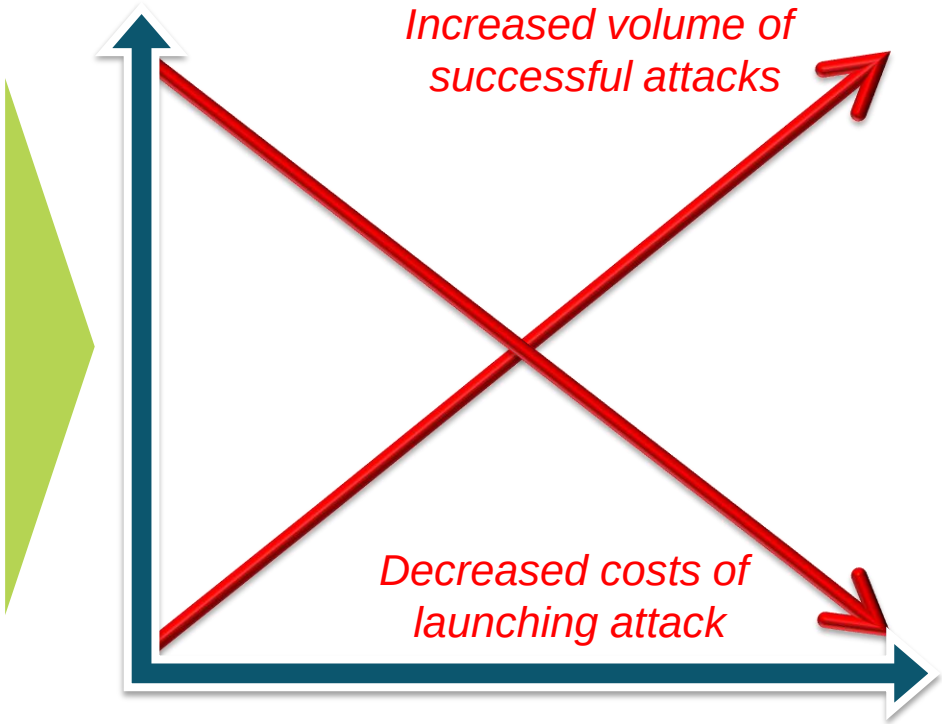


Economics of Attackers: Prevention Challenge

Increase in adversary skills and use of specialized tools

Innovation driving improved **attack toolkits**

Increase in number of **vulnerabilities & exploits**



Source: Ponemon Institute

THANK YOU!

dkriz@paloaltonetworks.com

www.paloaltonetworks.com

+1-571-266-5647

