CYBER SECURITY
EXECUTIVE

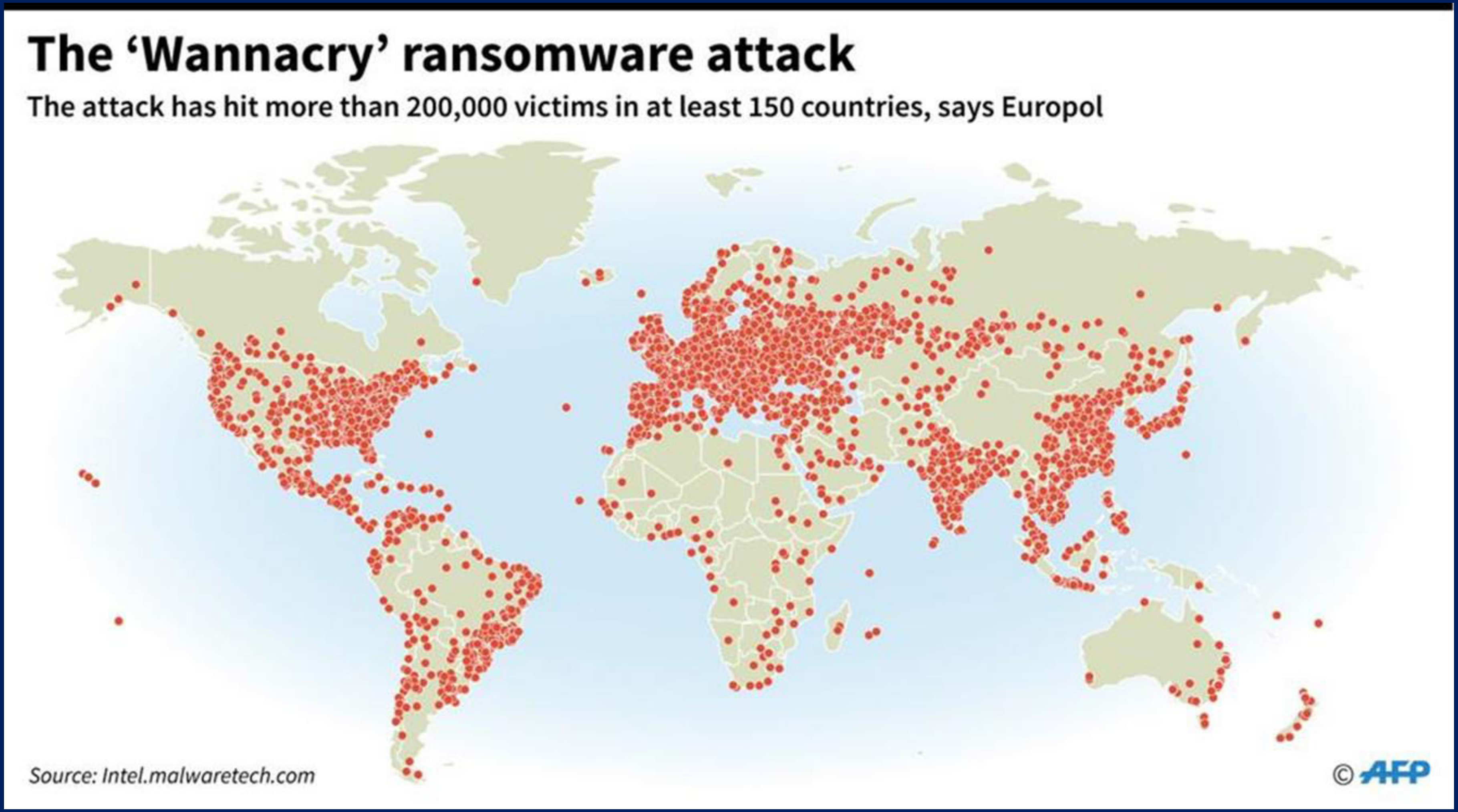
INFORMATION SHARING FOR OPTIMIZING CORPORATE CYBERSECURITY:

THE WHAT - THE WHY - THE HOW - THE WHO

Deborah Housen-Couriel, Adv.

November 13, 2018

WANNACRY – May 12-13, 2017



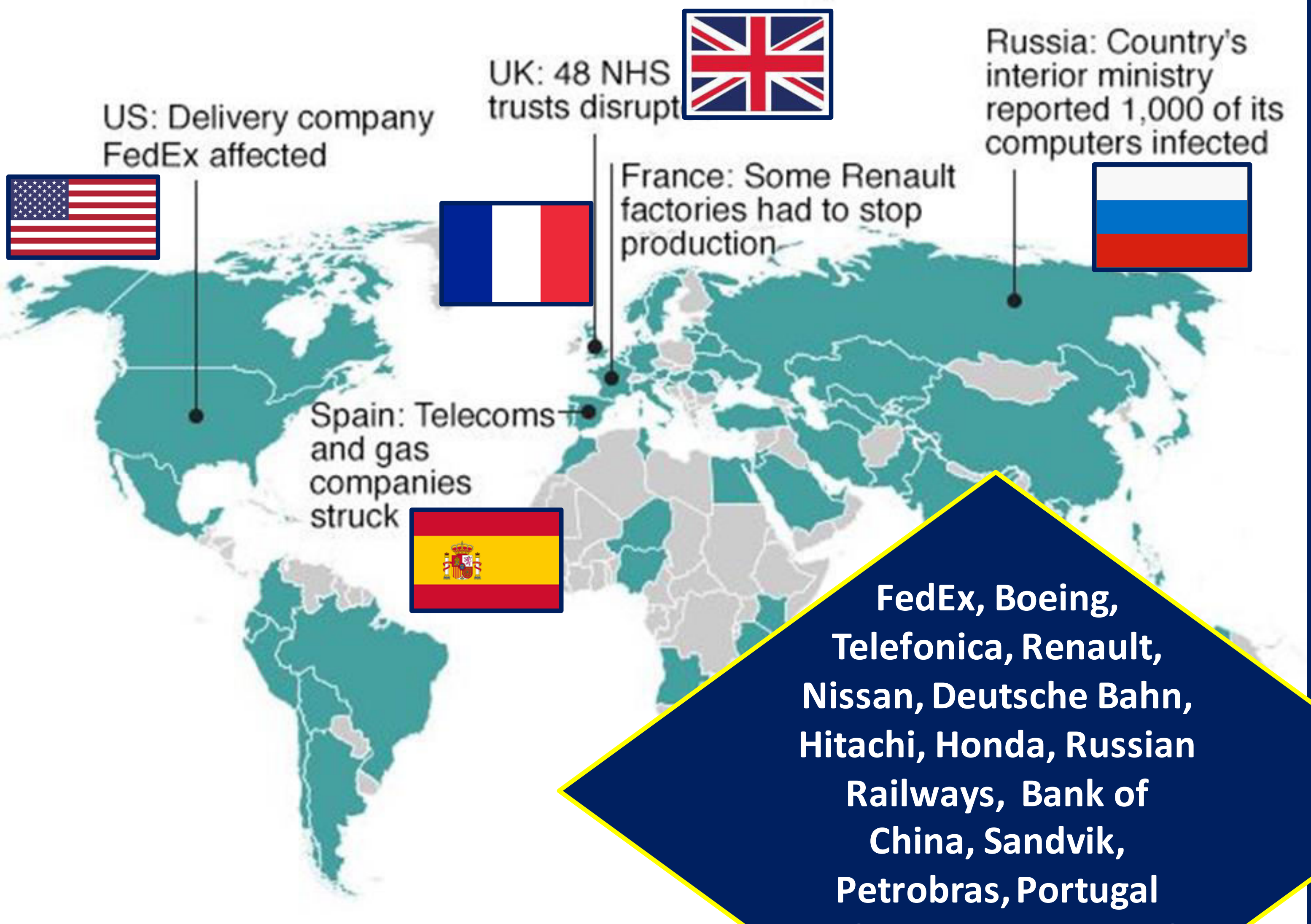
The ‘Wannacry’ ransomware attack

The attack has hit more than 200,000 victims in at least 150 countries, says Europol

Source: Intel.malwaretech.com

© AFP

Countries hit in initial hours of cyber-attack


US: Delivery company FedEx affected
UK: 48 NHS trusts disrupt
France: Some Renault factories had to stop production
Russia: Country's interior ministry reported 1,000 of its computers infected
Spain: Telecoms and gas companies struck

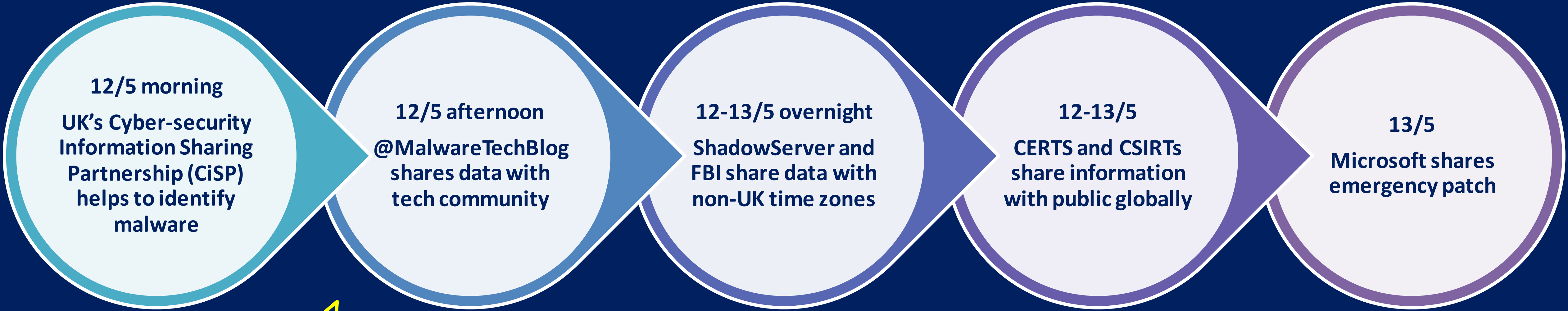
FedEx, Boeing, Telefonica, Renault, Nissan, Deutsche Bahn, Hitachi, Honda, Russian Railways, Bank of China, Sandvik, Petrobras, Portugal Telecom, UK National Health Service

*Map shows countries affected in first few hours o Kaspersky Lab research, as well as Australia, Swede idents have been reported since

Source: Kaspersky Lab's Global Research & Analysis Team

BBC

INFORMATION SHARING THAT MITIGATED WANNACRY



12/5 morning

UK's Cyber-security Information Sharing Partnership (CiSP) helps to identify malware

12/5 afternoon

@MalwareTechBlog shares data with tech community

12-13/5 overnight

ShadowServer and FBI share data with non-UK time zones

12-13/5

CERTS and CSIRTs share information with public globally

13/5

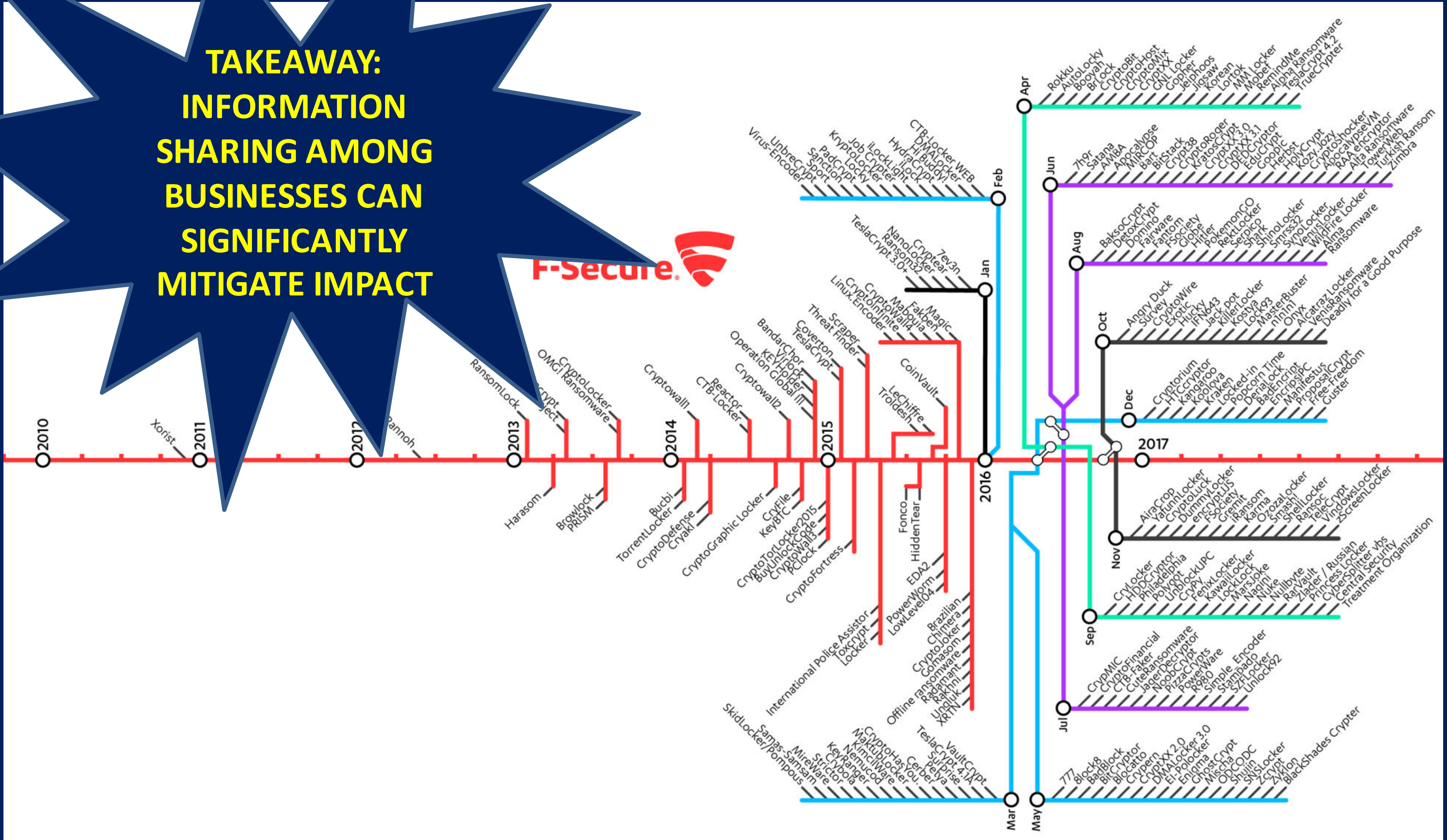
Microsoft shares emergency patch

14/4 Shadow Brokers leak an acquired NSA exploit Eternal Blue – not shared by the NSA, may have prevented WannaCry

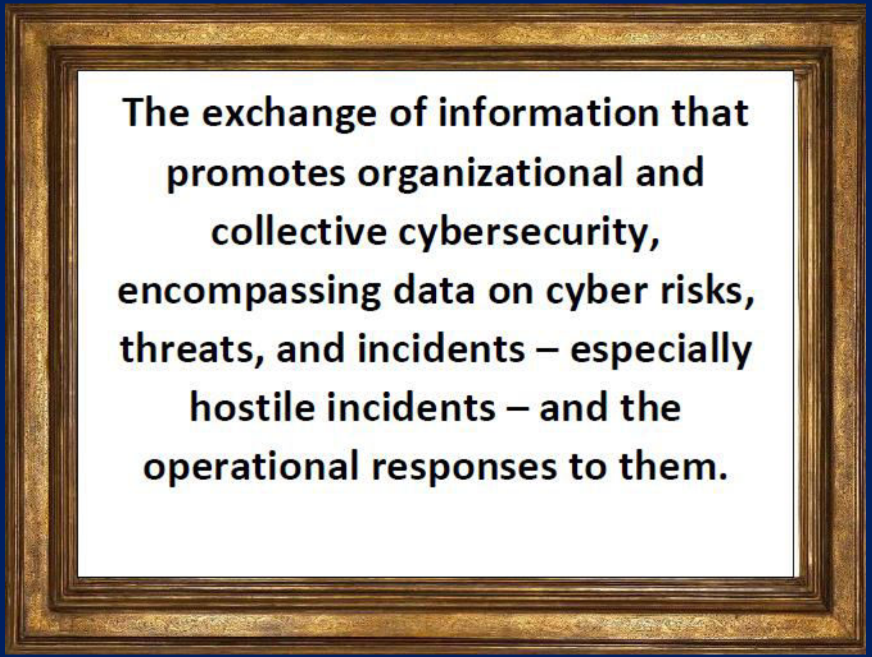
Marcus Hutchins

MALWARE ATTACKS ARE DRAMATICALLY INCREASING

TAKEAWAY: INFORMATION SHARING AMONG BUSINESSES CAN SIGNIFICANTLY MITIGATE IMPACT



WHAT'S INFORMATION SHARING?

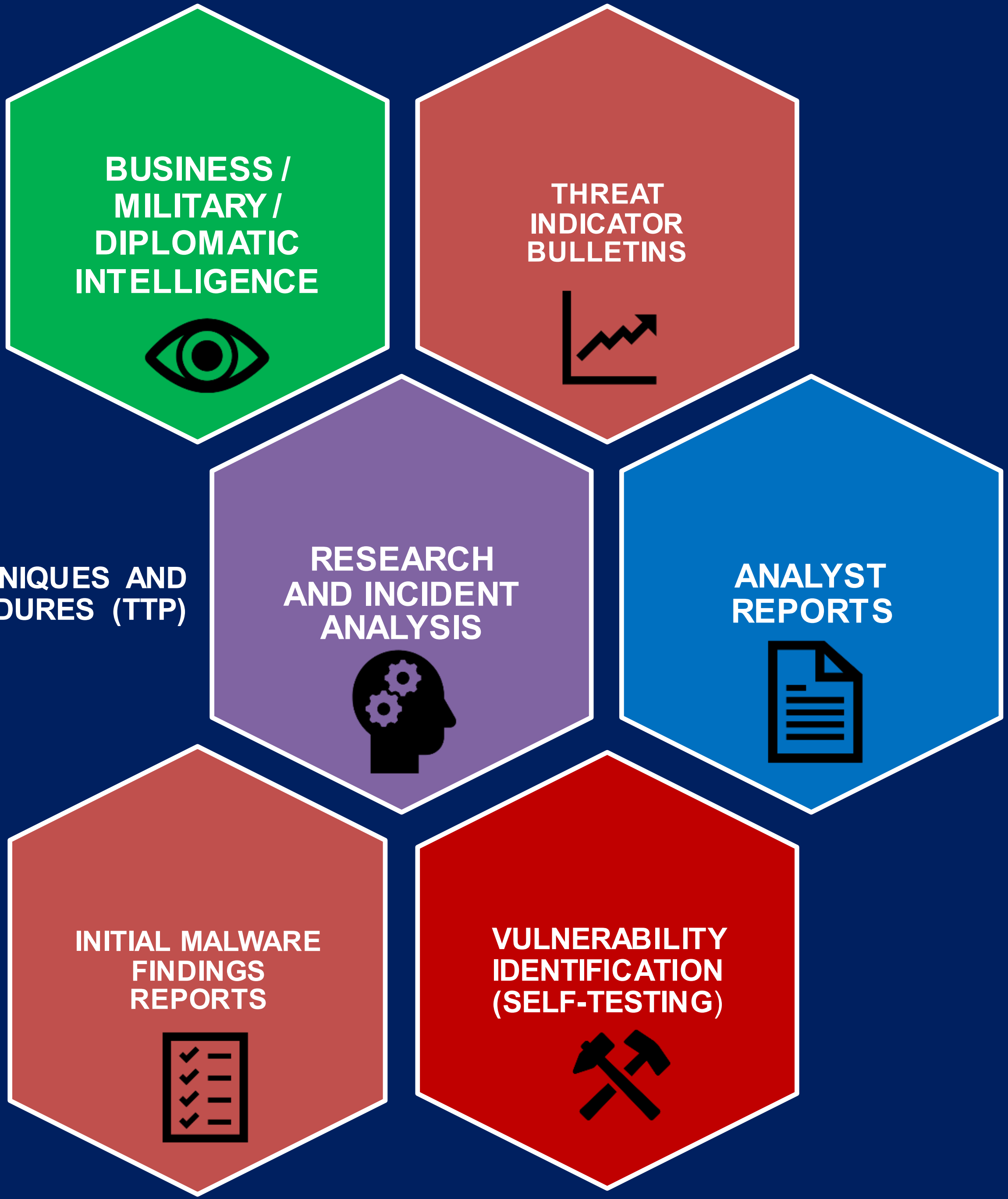


The exchange of information that promotes organizational and collective cybersecurity, encompassing data on cyber risks, threats, and incidents – especially hostile incidents – and the operational responses to them.

- Bridges gaps due to information asymmetries between attackers and their targets

- Identifies vulnerabilities of targeted organizations and the means to quickly mitigate exposures

- Reinforces shared best practices for cybersecurity



BUSINESS / MILITARY / DIPLOMATIC INTELLIGENCE

THREAT INDICATOR BULLETINS

TACTICS, TECHNIQUES AND PROCEDURES (TTP)

RESEARCH AND INCIDENT ANALYSIS

ANALYST REPORTS

BEST PRACTICES

INITIAL MALWARE FINDINGS REPORTS

VULNERABILITY IDENTIFICATION (SELF-TESTING)

WHY

The APT of information asymmetry between cyber attackers and their target organizations.

- No one organization has enough data for full situational awareness of the cyber threat landscape.

- Meet this challenge optimally by sharing cyber threat information among trusted partners in trusted communities.

- With IS, sharers achieve a more complete understanding of the threat landscape: strategically and tactically.

– Sean Barnum, 2014

INTER-
DEPENDENT
SECURITY

SPOILER ALERT- WHY IT'S CRITICAL FOR BUSINESSES TO SHARE INFORMATION (1)

- Governments won't solve this problem: we're stuck on **the normative project** to regulate cyberspace
  - **Clashing approaches:** US-EU-Russia-China standoff
  - **"You can't regulate trust":** Jan Neutze, Director of Cybersecurity Policy at Microsoft

SPOILER ALERT- WHY IT'S CRITICAL FOR BUSINESSES TO SHARE INFORMATION (2)

- Businesses need **pragmatic workarounds to manage cyber risk and invest strategically in cybersecurity**
  - IS has the potential to **significantly identify and mitigate cyber vulnerabilities for businesses** – but avoids normative gridlock
  - Better business **information and intelligence**
  - Optimal **corporate investment** in cybersecurity

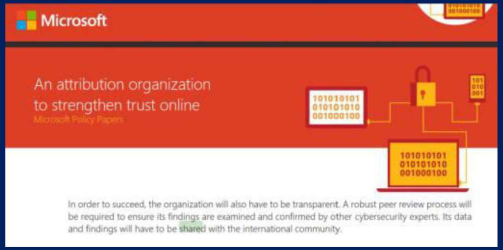
HOW

Specialized Trusted Platforms (STPs) for information sharing, where businesses are innovating with new and important initiatives for information sharing

CYBER THREAT ALLIANCE

European FI-ISAC

TECH ACCORD



Microsoft

An attribution organization to strengthen trust online

Microsoft Policy Papers

In order to succeed, the organization will also have to be transparent. A robust peer review process will be required to ensure its findings are examined and confirmed by other cybersecurity experts. Its data and findings will have to be shared with the international community.

GIFCT
Global Internet Forum
to Counter Terrorism

FINANCIAL SERVICES | Information Sharing and Analysis Center

CSIRTs NETWORK

tech against terrorism

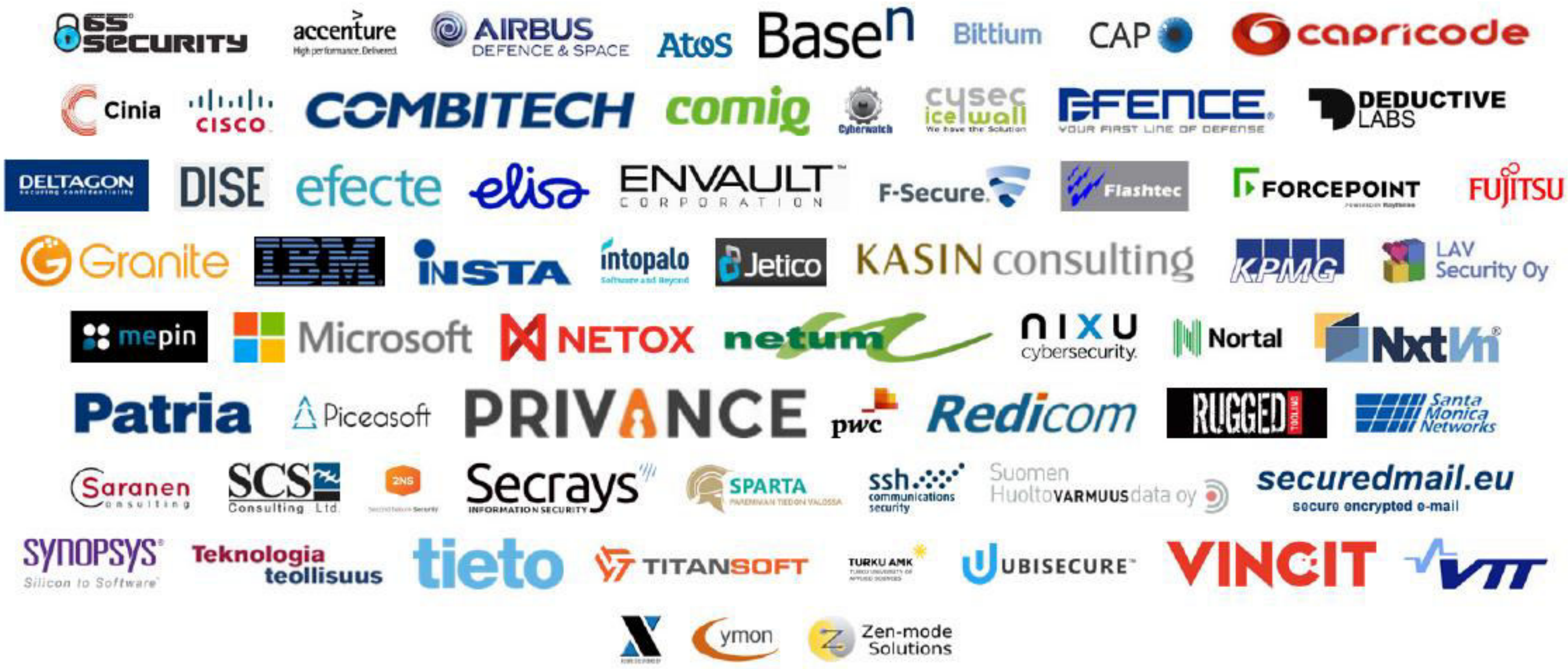
Launch
Knowledge Sharing Platform
The United Nations, New York
29th November 2017

Helping startups address the exploitation of their services

shadowserver

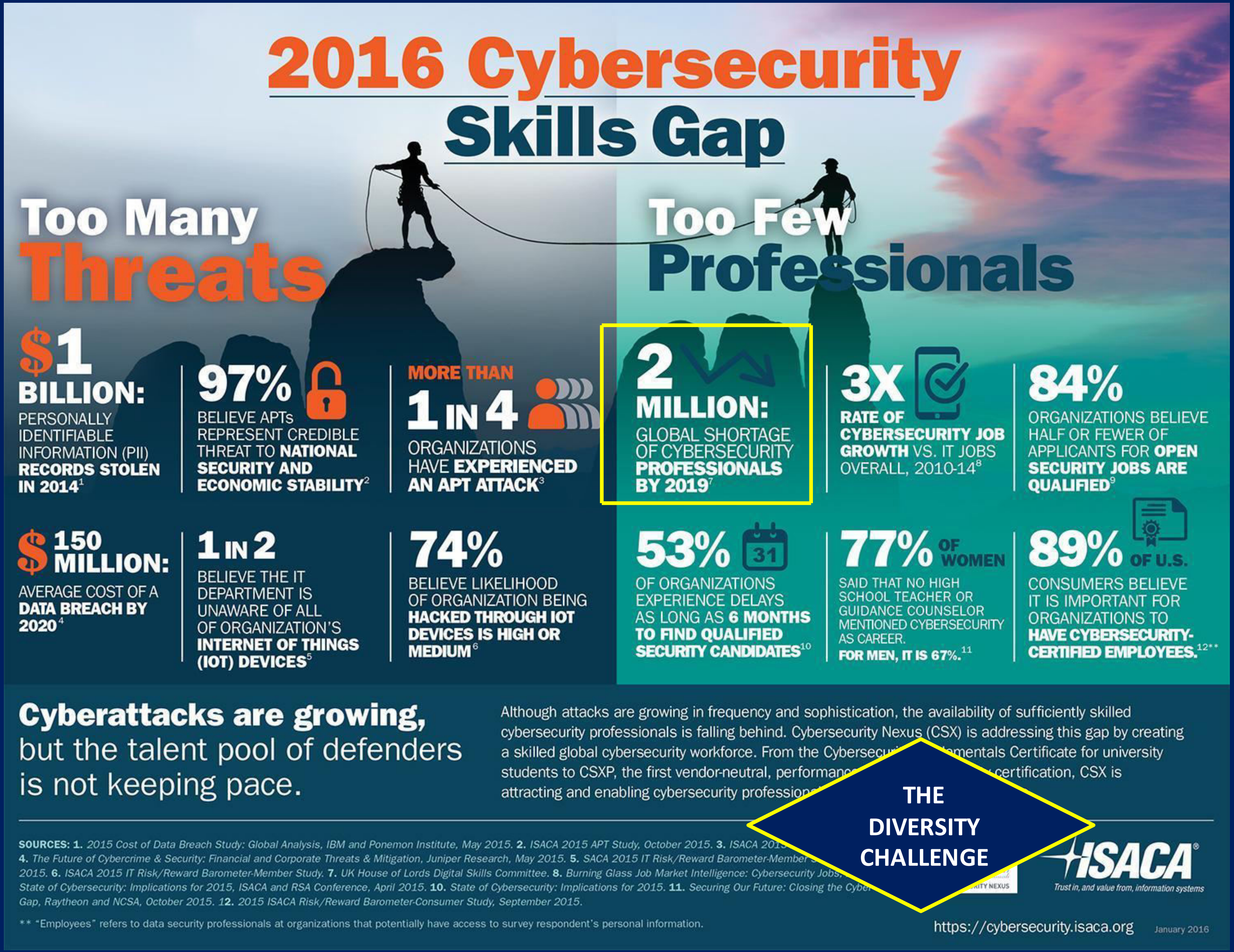
VirusTotal

FINNISH INFORMATION SECURITY CLUSTER



Finnish Information Security Cluster • Eteläranta 10, PL 10, 00131 Helsinki

WHO



2016 Cybersecurity Skills Gap

Too Many Threats

$1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) **RECORDS STOLEN IN 2014**[1]

97% BELIEVE APTs REPRESENT CREDIBLE THREAT TO **NATIONAL SECURITY AND ECONOMIC STABILITY**[2]

MORE THAN 1 IN 4 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[3]

$150 MILLION: AVERAGE COST OF A **DATA BREACH BY 2020**[4]

1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S **INTERNET OF THINGS (IOT) DEVICES**[5]

74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING **HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM**[6]

Too Few Professionals

2 MILLION: GLOBAL SHORTAGE OF CYBERSECURITY **PROFESSIONALS BY 2019**[7]

3X RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14[8]

84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR **OPEN SECURITY JOBS ARE QUALIFIED**[9]

53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS **6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES**[10]

77% OF WOMEN SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. **FOR MEN, IT IS 67%.**[11]

89% OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO **HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.**[12**]

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecu lementals Certificate for university students to CSXP, the first vendor-neutral, performanc certification, CSX is attracting and enabling cybersecurity profession

SOURCES: 1. *2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015.* **2.** *ISACA 2015 APT Study, October 2015.* **3.** *ISACA 201* **4.** *The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, Juniper Research, May 2015.* **5.** *SACA 2015 IT Risk/Reward Barometer-Member* *2015.* **6.** *ISACA 2015 IT Risk/Reward Barometer-Member Study.* **7.** *UK House of Lords Digital Skills Committee.* **8.** *Burning Glass Job Market Intelligence: Cybersecurity Jobs,* *State of Cybersecurity: Implications for 2015, ISACA and RSA Conference, April 2015.* **10.** *State of Cybersecurity: Implications for 2015.* **11.** *Securing Our Future: Closing the Cyber* *Gap, Raytheon and NCSA, October 2015.* **12.** *2015 ISACA Risk/Reward Barometer-Consumer Study, September 2015.*

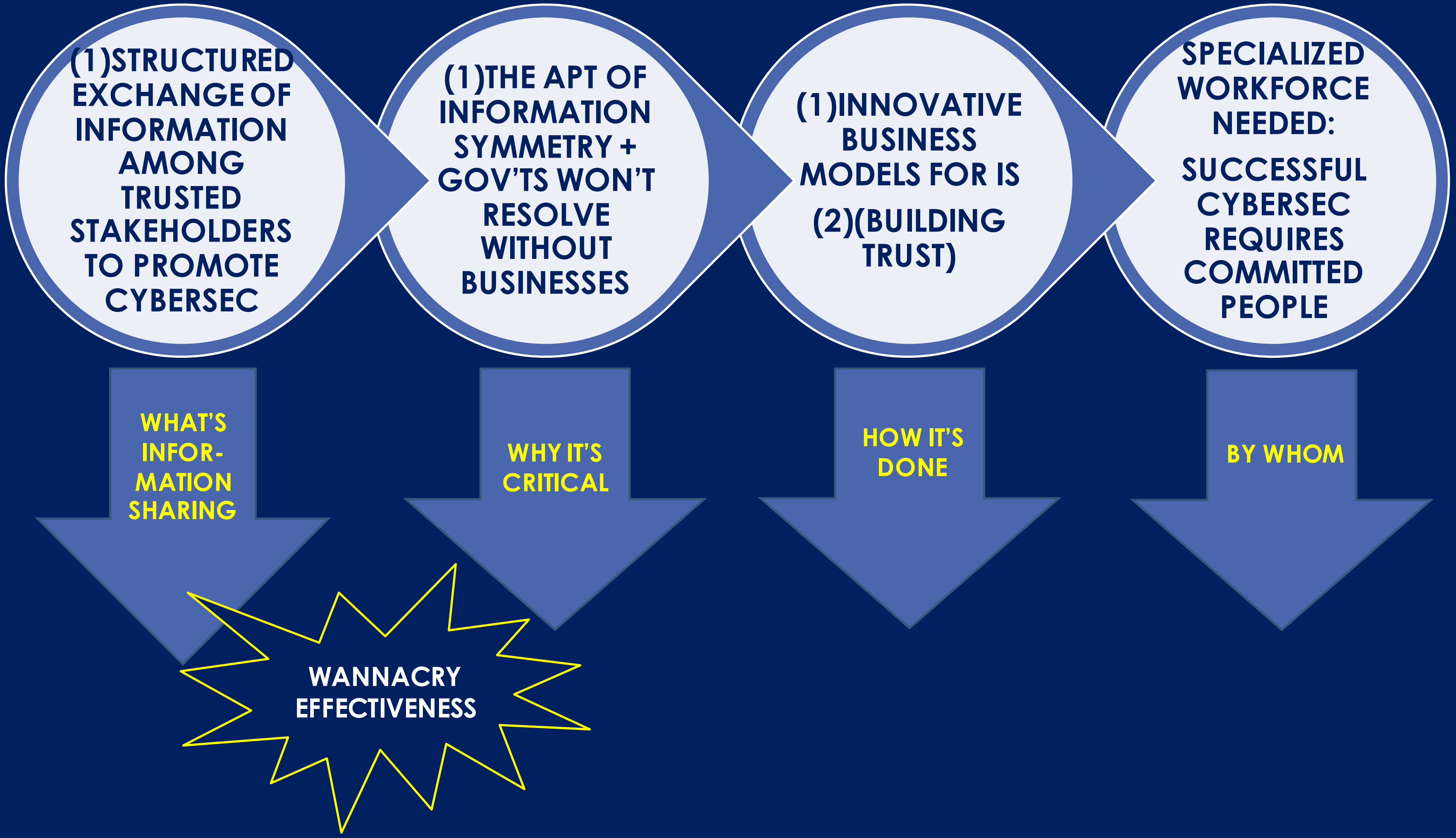
** "Employees" refers to data security professionals at organizations that potentially have access to survey respondent's personal information.

https://cybersecurity.isaca.org

January 2016

THE DIVERSITY CHALLENGE

WRAPPING UP



(1)STRUCTURED EXCHANGE OF INFORMATION AMONG TRUSTED STAKEHOLDERS TO PROMOTE CYBERSEC

(1)THE APT OF INFORMATION SYMMETRY + GOV'TS WON'T RESOLVE WITHOUT BUSINESSES

(1)INNOVATIVE BUSINESS MODELS FOR IS

(2)(BUILDING TRUST)

SPECIALIZED WORKFORCE NEEDED:

SUCCESSFUL CYBERSEC REQUIRES COMMITTED PEOPLE

WHAT'S INFORMATION SHARING

WHY IT'S CRITICAL

HOW IT'S DONE

BY WHOM

WANNACRY EFFECTIVENESS

3 TAKEAWAYS

KIITOS.

deborah@cyberregstrategies.com

Information sharing is evolving in innovative ways:

USE IT to manage your business' risk!

Be selective about your choice of sharing platforms

Prioritize the buildup of your cybersecurity workforce, leveraging IS to improve it

BOTTOM LINE: INFORMATION SHARING IS CRITICAL FOR MANAGING YOUR BUSINESS' CYBER RISK AND CYBERSECURITY INVESTMENT