



CYBERSECURITY IN THE GLOBAL FINANCIAL SECTOR: REGULATION OF INFORMATION SHARING AS A CRITICAL ELEMENT

**Deborah Housen-Couriel, Adv.
June 23, 2019, 11:00-12:00**



THE FEDERMANN
CYBER SECURITY CENTER
Cyber Law Program



האוניברסיטה העברית בירושלים
THE HEBREW UNIVERSITY OF JERUSALEM

The Federmann Cyber Security Center – Cyber Law Program



ISRAEL BAR ASSOCIATION
לשכת עורכי הדין בישראל
نقابة المحامين في إسرائيل

WELLESLEY
W



פורום דבורה
Forum Dvorah

נשים כמדיניות חוץ ונבחנות לאומי



HARVARD
Kennedy
School

KONFIDAS
Your business, secured.

WANNACRY – May 12-13, 2017

The 'Wannacry' ransomware attack

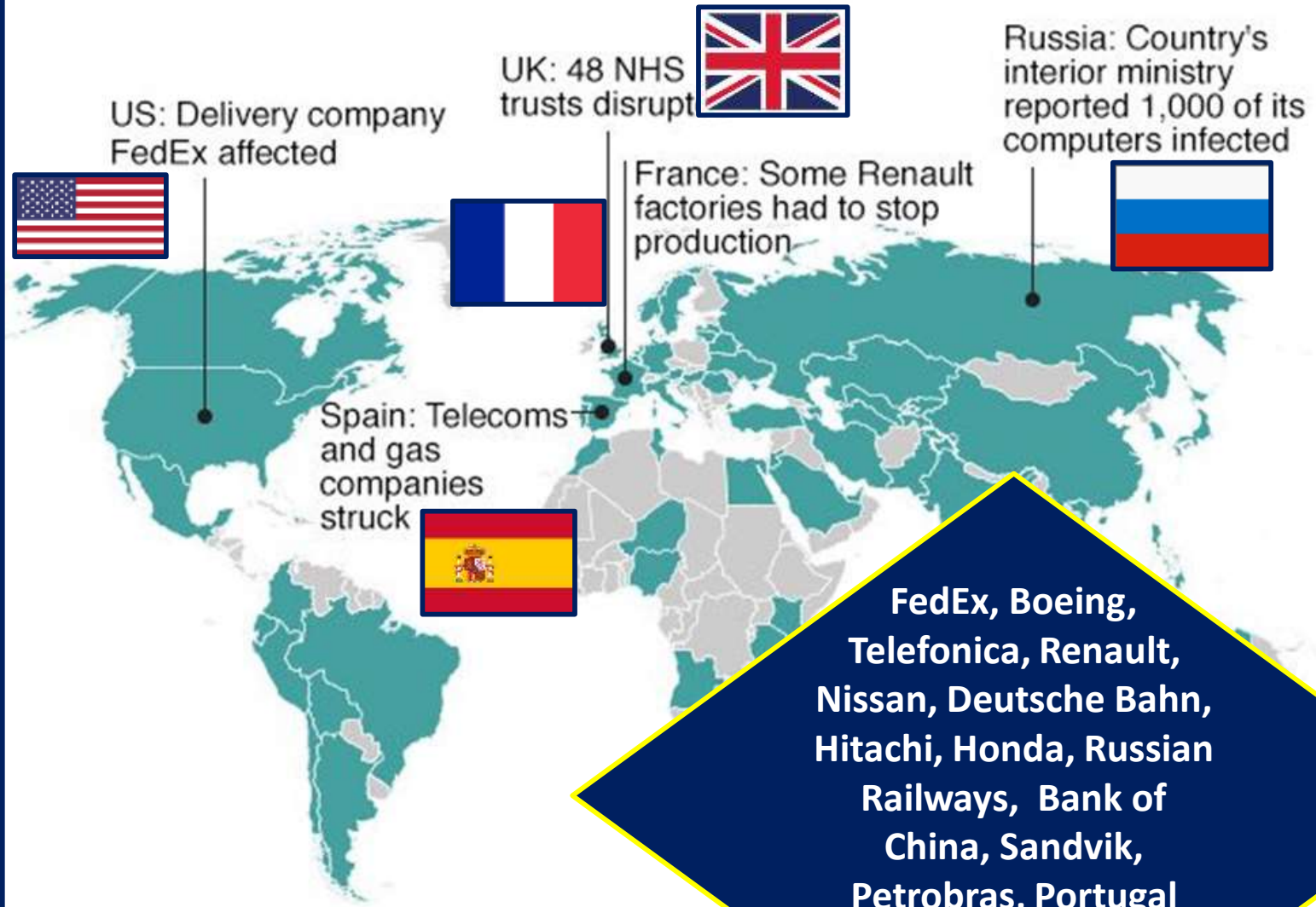
The attack has hit more than 200,000 victims in at least 150 countries, says Europol



Source: Intel.malwaretech.com

© AFP

Countries hit in initial hours of cyber-attack



*Map shows countries affected in first few hours of attack, according to Kaspersky Lab research, as well as Australia, Sweden, and others. Incidents have been reported since

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

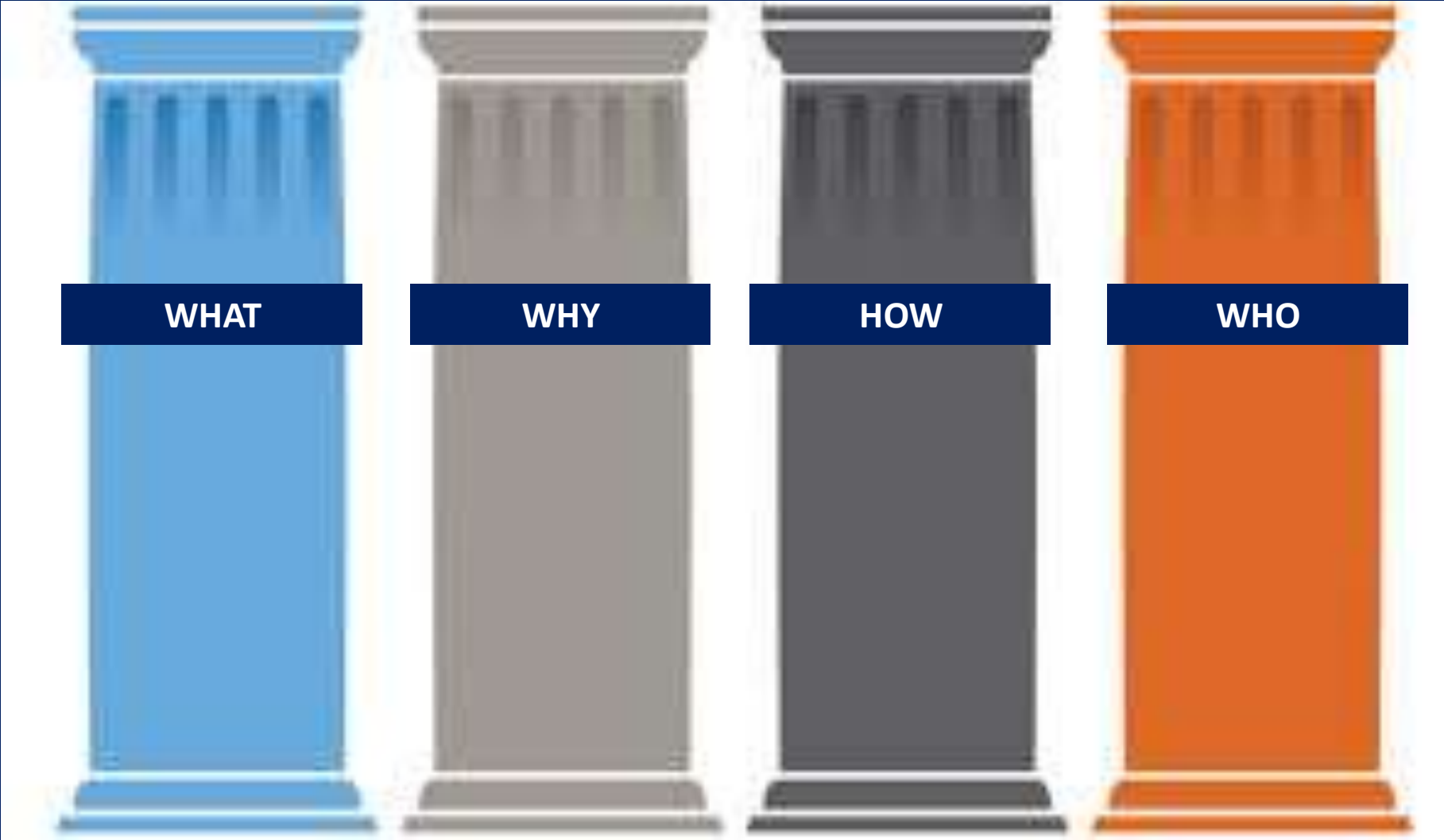
13/5
Microsoft shares
emergency patch

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



Marcus Hutchins





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

- Governments won't solve this problem alone: we're stuck on **the normative project** to regulate cyberspace
 - **Clashing approaches:** US-EU-Russia-China standoff (UN 2019)
 - **“You can't regulate trust”:** Jan Neutze, Director of Cybersecurity Policy at Microsoft

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

- Businesses and govt's 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 **information and intelligence**



- Optimal **corporate / gov't investment** in cybersecurity



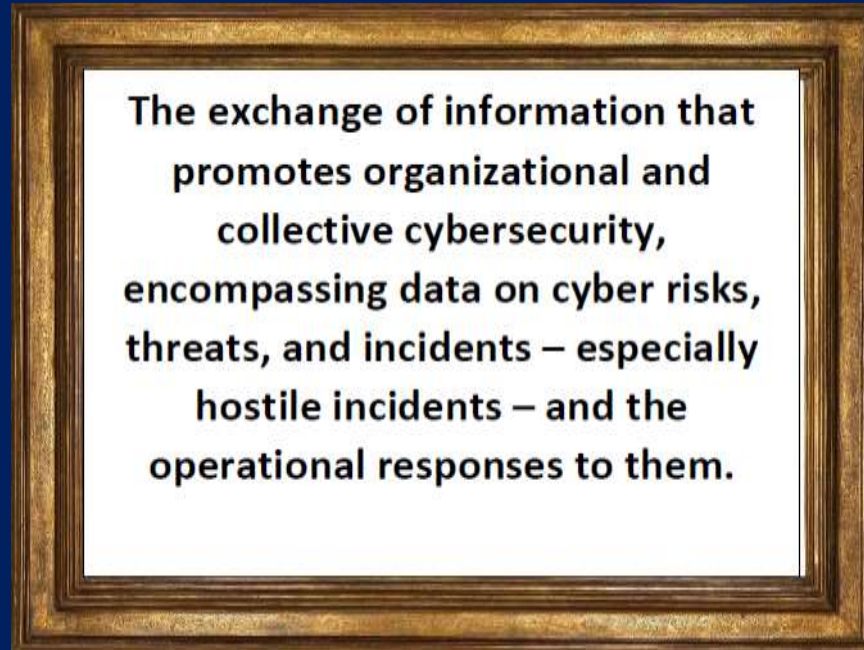
SPOILER ALERT- WHY IT'S CRITICAL FOR BUSINESSES AND GOVT'S TO SHARE CYBER INFORMATION (3)

- Information sharing is **especially critical for the financial sector:**
 - **Underlying critical infrastructure** nationally, regionally, globally
 - High **interdependence** in cyberspace – only increasing
 - Trans-national **risks and vulnerabilities**
 - The **“weakest link”** problem



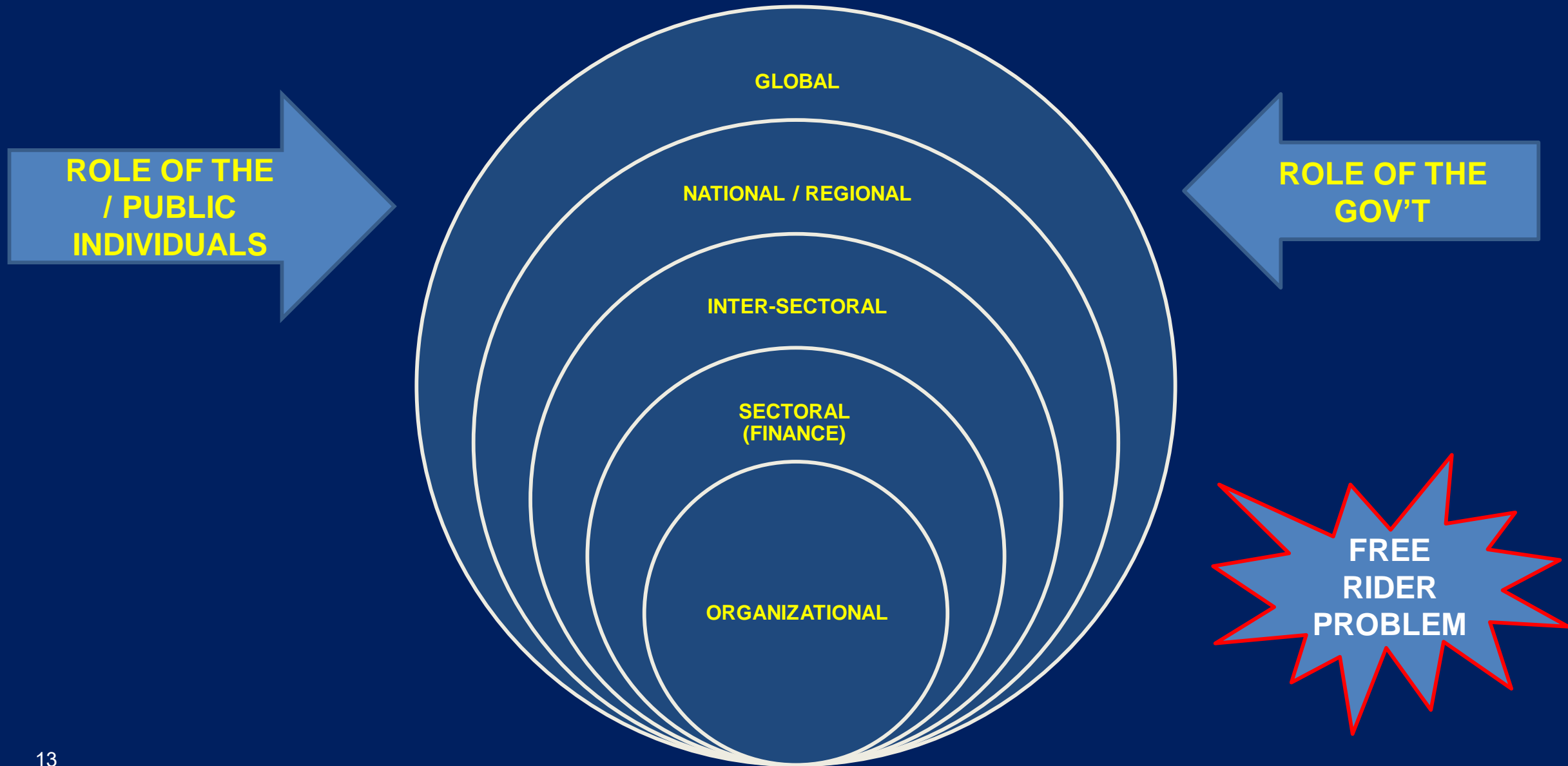
WEF GLOBAL RISKS REPORT 2019 - The Global Risks Landscape

WHAT'S INFORMATION SHARING?



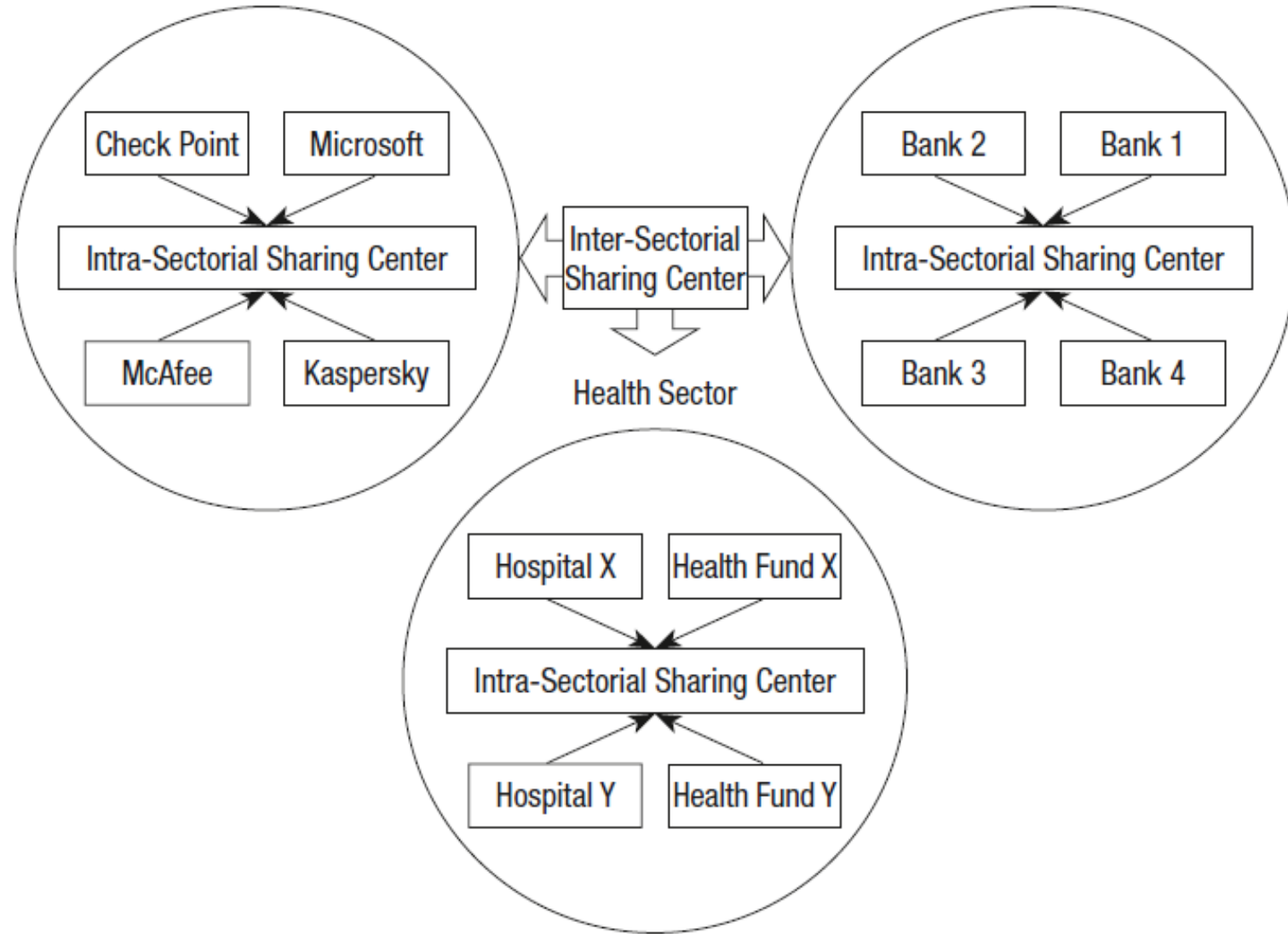
- Bridges gaps due to **information asymmetries** between attackers and their targets
- Identifies **vulnerabilities** of targeted organizations and the means to quickly **mitigate exposures**
- Reinforces shared **best practices** for cybersecurity

OPTIMALLY – NESTED *MODUS OPERANDI* FOR IS



Information Security Solutions Sector

Financial Sector





Example #1: EU Network and Information Security Directive, 2016

Article 1

Subject matter and scope

1. This Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.

2. To that end, this Directive:
 - (c) ~~creates a computer security incident response teams network~~ ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation,

 - (e) lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

Example #1: EU Network and Information Security Directive, 2016 (2)

6. This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular to safeguard national security, including actions protecting information the disclosure of which Member States consider contrary to the essential interests of their security, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences.

Example #2: Ceres and SWIFT



FS-ISAC sets up global cyber forum for central banks and regulatory authorities

11 June 2018



Central banks and regulators are to share information and intelligence on emerging cyber-threats through a new forum established under the aegis of the Financial Services Information Sharing and Analysis Center (FS-ISAC).

FS-ISAC was established in 1999 to share threats and vulnerability information among its 7000-strong community of banks, credit unions, insurance companies, investment companies and other financial institutions.

Swift launches cyber-threat intelligence service

15 May 2017



Interbank co-operative Swift has launched an 'Information Sharing and Analysis Centre' to provide member banks with timely intelligence on the latest trends in cyber-security.

SWIFT ISAC PORTAL TERMS OF USE, April 2018

The SWIFT ISAC portal (the “Portal”) is a dedicated part of swift.com through which SWIFT shares information related to security threats potentially impacting our customers.

SWIFT has created the Portal for use by SWIFT users and customers. In limited instances, SWIFT may determine that it is appropriate to grant access to the Portal to business firms and other entities (always excluding natural persons) that are not SWIFT users or customers (such firms and entities are collectively referred to as “Third Parties”). The decision to grant or deny such access is solely within SWIFT’s discretion. SWIFT reserves the right to terminate any Third Party’s access to the Portal for any reason SWIFT deems appropriate.

When used in these Terms of Use, “information” means information of any nature or in any form communicated through the Portal, including, but not limited to, indicators of compromise, information about modus operandi, knowledge based tips, reports, incident reports, bulletins and the like.

SWIFT DISCLAIMER: IS “AS IS” (2)

Information may include general guidelines, recommendations or interpretation of data. The recipient is solely and exclusively responsible for deciding any particular course of action or omission and for analyzing and/or implementing any actions or taking any decision on this basis. Nothing with respect to shared information shall be interpreted or construed as constituting any obligation, representation or warranty on the part of SWIFT. The provision by SWIFT of information cannot be considered to constitute any assumption or admission of involvement, liability or responsibility for any security incident, cyber-attack, modus operandi, or indicator of compromise described or referred to therein.

Example #3: ISRAEL'S CF3



Ministry of Finance

(/en)

משרד האוצר

Cyber and Finance Continuity Center

The Cyber and Finance Continuity Center (FC3) was established in January 2017, as part of cooperation between the Cyber, Emergency and Security Division in the Ministry of Finance and the Cyber Directorate in the Prime Minister's office.

The mission of FC3, as an integral part of the Israeli CERT, the NCSA, and the ministry of finance is to ensure business continuity and financial services availability to the public and the government while projecting confidence, stability and financial leadership. In addition, FC3 is responsible for strengthening the resiliency of the financial services sector against attacks and other threats to the Israeli financial sector by proactively identifying threats and promoting protection, driving preparedness, and collaborating with worldwide financial institutions.



Example #3: ISRAEL'S CF3 (2)

The center focuses on the following key financial processes: cash flow, credit card operations, allowance payments and stock exchange trading.

The Cyber and Finance Continuity Center provides the following services to its members:

1. Increase the Israeli cyber financial resilience;
2. Provide a platform and encourage information sharing and cooperation among the financial institutions;
3. Provide situation analysis for the decision makers; and
4. Operate response teams and provide incident handling.

Supervisor of Banks: Proper Conduct of Banking Business Directive 361 (03/15) [1]
Cyber Defense Management

Cyber Defense Management

ARTICLES 24,26,31, 55, 60, 64-67

Example #3: ISRAEL'S CF3 (3)

Information and Intelligence Sharing

64. The banking corporation shall gather and analyze relevant information from internal and external sources, for the purpose of creating a comprehensive and current perception of the cyber threat landscape and the banking corporation's exposure to it. This information shall be used as a basis for a knowledgeable decision making, prioritizing modes of operation, and maintaining real time effective defense.
65. The threat and vulnerability landscape shall be derived *inter alia* from the following information: mapping of relevant threat factors, with respect to motivation and capabilities; techniques, tactics, scenarios and attack tools; weaknesses, system configurations and/or vulnerabilities that could be exploited for attacks; attacks that occurred in the past (at the

Example #3: ISRAEL'S CF3 (4)

banking corporation and/or in its operational environment); response actions taken in the past, means and indicators for detecting and identifying attacks and handling them.

66. The banking corporation shall share information that may help other banking corporations in handling cyber threats.
67. Information shall be gathered and shared in accordance with the directives of the Supervisor of Banks, and the applicable law.

Israel Cybersecurity Landscape: Israel CyberSlide®

September 2018



Silver Sponsors: CYBERBIT, CYMULATE, XM CYBER, illusive, Cy-oT

Gold Sponsors: SC

info@cyberstartupobservatory.com

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



By exchanging cyber threat information within a sharing community, organizations can **leverage the collective knowledge, experience, and capabilities** of that sharing community to gain **a more complete understanding of the threats** the organization may face. Using this knowledge, *an organization can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies.* By correlating and analyzing cyber threat information from multiple sources, an organization can also **enrich existing information and make it more actionable.**

BARRIERS TO IS

- Despite the advantages that IS can bring to private sector entities for the mitigation of cyber risk due to information asymmetries, **financial services organizations often fail to fully adopt and internalize IS** for reasons that may be characterized as either **(a) operative** or **(b) normative-substantive**.

BARRIERS TO IS: OPERATIVE

- ***The inability to establish trust*** among sharing entities (some of whom may be competitors);
- ***Costs related to IS*** including (a) recruitment, training and retention of appropriate cybersecurity personnel and (b) organizational time spent on IS, including time devoted to “false positives” when IS is less than optimal;
- ***Lack of transparency regarding the robustness and confidentiality of IS platforms***, including the use of shared data by any participating government agencies for non-cybersecurity purposes;
- ***Regulatory redundancy***, where other, possibly competing IS formats are mandated and may complicate efficient IS;

BARRIERS TO IS: NORMATIVE

- *The **potential exposure of protected personal data*** held by the organization, including a lack of statutory limitation on the purposes of the government regulator's use of such data; non-transparent sharing via government channels with agencies and actors, including those outside of IS jurisdiction; and data breaches impacting the IS platforms themselves;
- *The **potential exposure of organizational IP***, with potential chilling effects on organizational innovation; and possible implications for corporate market value.

•

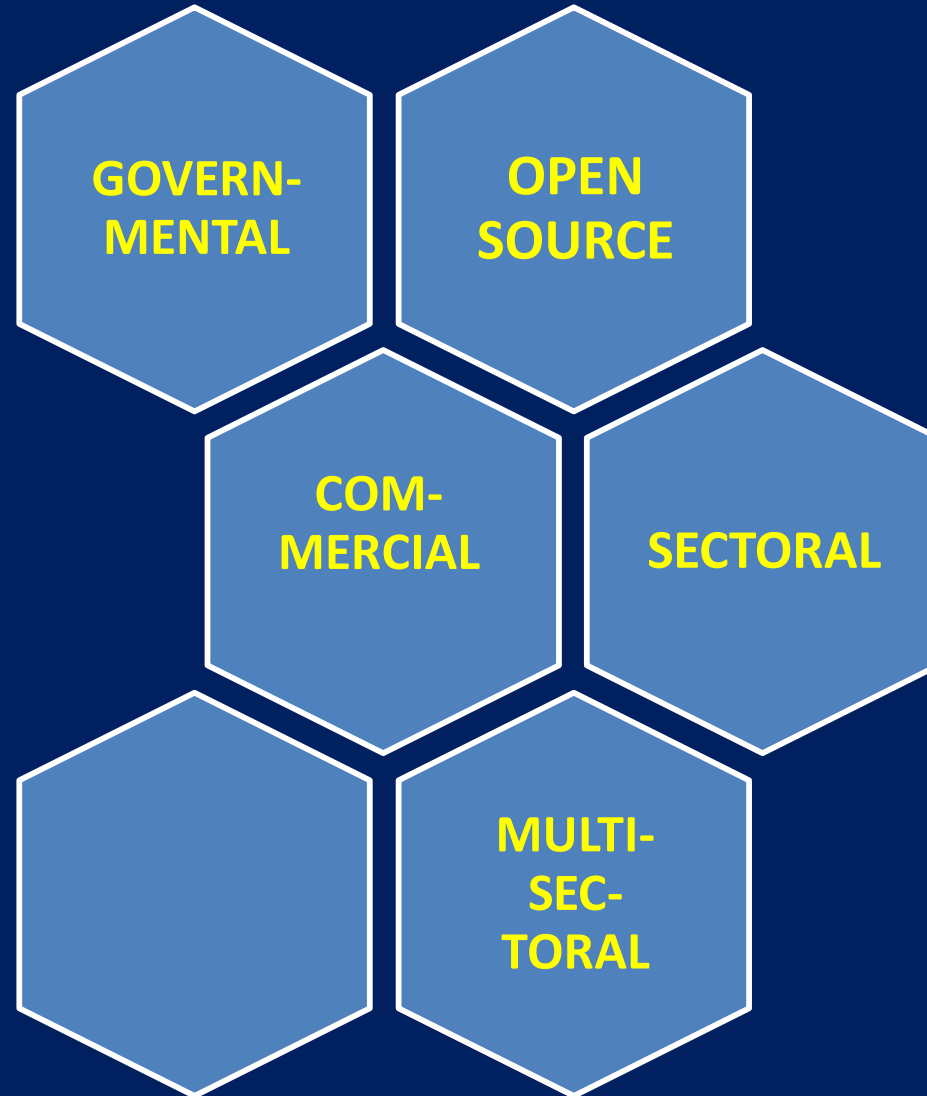
•

HOW

Specialized Trusted Platforms (STPs) for information sharing, where govt's businesses are innovating with new initiatives for IS



TYPES



Name	Type	Year	Owner	Project site(s)
Collaborative Research Into Threats (CRITs)	Open Source	2014	MITRE	https://crits.github.io/ https://github.com/crits
Collective Intelligence Framework (CIF)	Open Source	2012	CSIRT Gadgets Foundation	http://csirtgadgets.org/ https://github.com/csirtgadgets
GOSINT	Open Source	2017	Cisco	https://github.com/ciscocsirt/GOSINT https://gosint.readthedocs.io/en/latest/
MANTIS Cyber Threat Intelligence Management Framework	Open Source	2013	SIEMENS	https://django-mantis.readthedocs.io/en/latest/ https://github.com/siemens/django-mantis
Malware Information Sharing Platform (MISP)	Open Source / Community	2012	CIRCL	http://www.misp-project.org/ https://github.com/MISP https://www.misp-project.org/communities/
MineMeld	Open Source	2016	Palo Alto	https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/minemeld https://github.com/PaloAltoNetworks/minemeld
Yeti	Open Source	2017	Yeti	https://yeti-platform.github.io/ https://github.com/yeti-platform
ThreatStream	Commercial	2013	Anomali	https://www.anomali.com/platform
EclecticIQ Platform	Commercial	2014	EclecticIQ	https://www.eclecticiq.com/platform
LookingGlass	Commercial	2015	LookingGlass	https://www.lookingglasscyber.com/products/manage-intelligence/
Soltra Edge	Commercial	2014	NC4	https://www.soltra.com/en/
Threat Central	Community	2015	Micro Focus	https://software.microfocus.com/en-us/software/cyber-threat-analysis
ThreatConnect	Commercial	2013	ThreatConnect	https://www.threatconnect.com/
ThreatQ Platform	Commercial	2015	ThreatQuotient	https://www.threatq.com/threatq/
TruSTAR	Commercial	2014	TruSTAR Technologies	https://trustar.co/
Open Threat Exchange (OTX)	Community	2012	AlienVault	https://www.alienvault.com/open-threat-exchange
ThreatExchange	Community	2015	Facebook	https://developers.facebook.com/products/threat-exchange
X-Force Exchange	Community	2015	IBM	https://exchange.xforce.ibmcloud.com/

Waterholing attack on financial websites Campaign

✎ Edit

N New Investigation

✖ Delete

"On 3rd February 2017, researchers at badcyber.com released an article that detailed a series of attacks directed at Polish financial institutions. The article is brief, but states that "This is – by far – the most serious information security incident we have seen in Poland" followed by a claim that over 20 commercial banks had been confirmed as victims."

References:

- <https://baesystemsai.blogspot.fr/2017/02/lazarus-watering-hole-attacks.html>
- <http://baesystemsai.blogspot.fr/2017/02/lazarus-false-flag-malware.html>
- <https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0>
- <http://www.welivesecurity.com/2017/02/16/demystifying-targeted-malware-used-polish-banks/>
- <http://blog.trendmicro.com/trendlabs-security-intelligence/ratankba-watering-holes-against-enterprises/>

Info

Tags

waterholing_eye-watch

Aliases

Files

No files for now.

Choisissez un fichier

Aucun fichier choisi

Attach

TTP

Malware

Actors

Campaigns

Exploits

ExploitKits

Indicators

Observables

Prev

Page 1

Next

tags=evil

Filter

Timeframe	Link	Value	Tags	Context	Creation date
2017-03-15 - 2017-03-15	Tagged	movis-es.ignorelist.com	waterholing_eye-watch c2		2017-03-15 21:02
2017-03-15 - 2017-03-15	Tagged	tradeboard.mefound.com	waterholing_eye-watch c2		2017-03-15 21:02
2017-03-15 - 2017-03-15	Tagged	krf.gov.pl	compromised waterholing_eye-watch		2017-03-15 20:38

Tip: Click on table rows to select them

Easily track campaigns, related observables, malware, actors

[About CISA](#)[Cybersecurity](#)[Infrastructure Security](#)[Emergency Communications](#)[National Risk Management](#)[News & Media](#)

[Home](#) > [CISA](#) > [Cybersecurity](#) > [Information Sharing](#) > [Cyber Information Sharing and Collaboration Program \(CISCP\)](#)

[Share / Email](#) 

Information Sharing

[Automated Indicator Sharing \(AIS\)](#)

[Cyber Information Sharing and Collaboration Program \(CISCP\)](#)





[Enhanced Cybersecurity Services](#)

[Information Sharing and Analysis Organizations](#)

[National Cybersecurity & Communications Integration Center](#)

Cyber Information Sharing and Collaboration Program (CISCP)

The U.S. Department of Homeland Security (DHS) Cyber Information Sharing and Collaboration Program (CISCP) enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure (CI) sectors. CISCP fosters this collaboration by leveraging the depth and breadth of DHS cybersecurity capabilities within a focused operational context. Through analyst-to-analyst sharing of threat and vulnerability information, CISCP helps partners manage cybersecurity risks and enhances our collective ability to proactively detect, prevent, mitigate, respond to, and recover from cybersecurity incidents. CISCP's overall objective is to build cybersecurity

Color	When should it be used?	How may it be shared?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>

Structured Threat Information Expression (STIX), Cyber Observable Expression (CybOX)

WHO



2016 Cybersecurity Skills Gap

Too Many Threats

Too Few Professionals

\$1 BILLION:
PERSONALLY IDENTIFIABLE INFORMATION (PII) RECORDS STOLEN IN 2014¹

97% BELIEVE APTs REPRESENT CREDIBLE THREAT TO NATIONAL SECURITY AND ECONOMIC STABILITY²

MORE THAN 1 IN 4 ORGANIZATIONS HAVE EXPERIENCED AN APT ATTACK³

2 MILLION:
GLOBAL SHORTAGE OF CYBERSECURITY PROFESSIONALS BY 2019⁴

3X RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14⁵

84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR OPEN SECURITY JOBS ARE QUALIFIED⁶

\$150 MILLION:
AVERAGE COST OF A DATA BREACH BY 2020⁷

1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S INTERNET OF THINGS (IOT) DEVICES⁸

74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM⁹

53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS 6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES¹⁰

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.

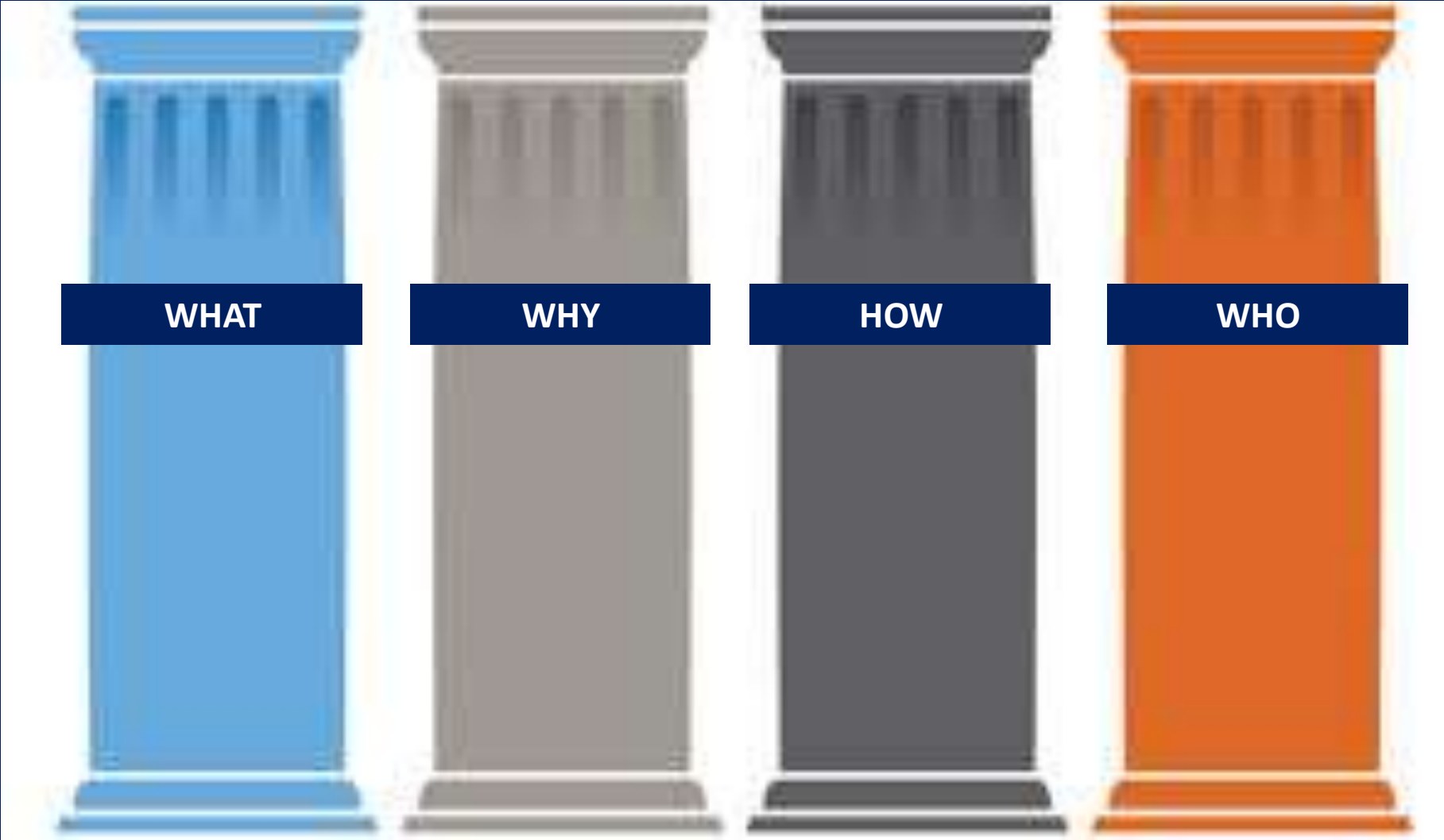
Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate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

THE DIVERSITY CHALLENGE

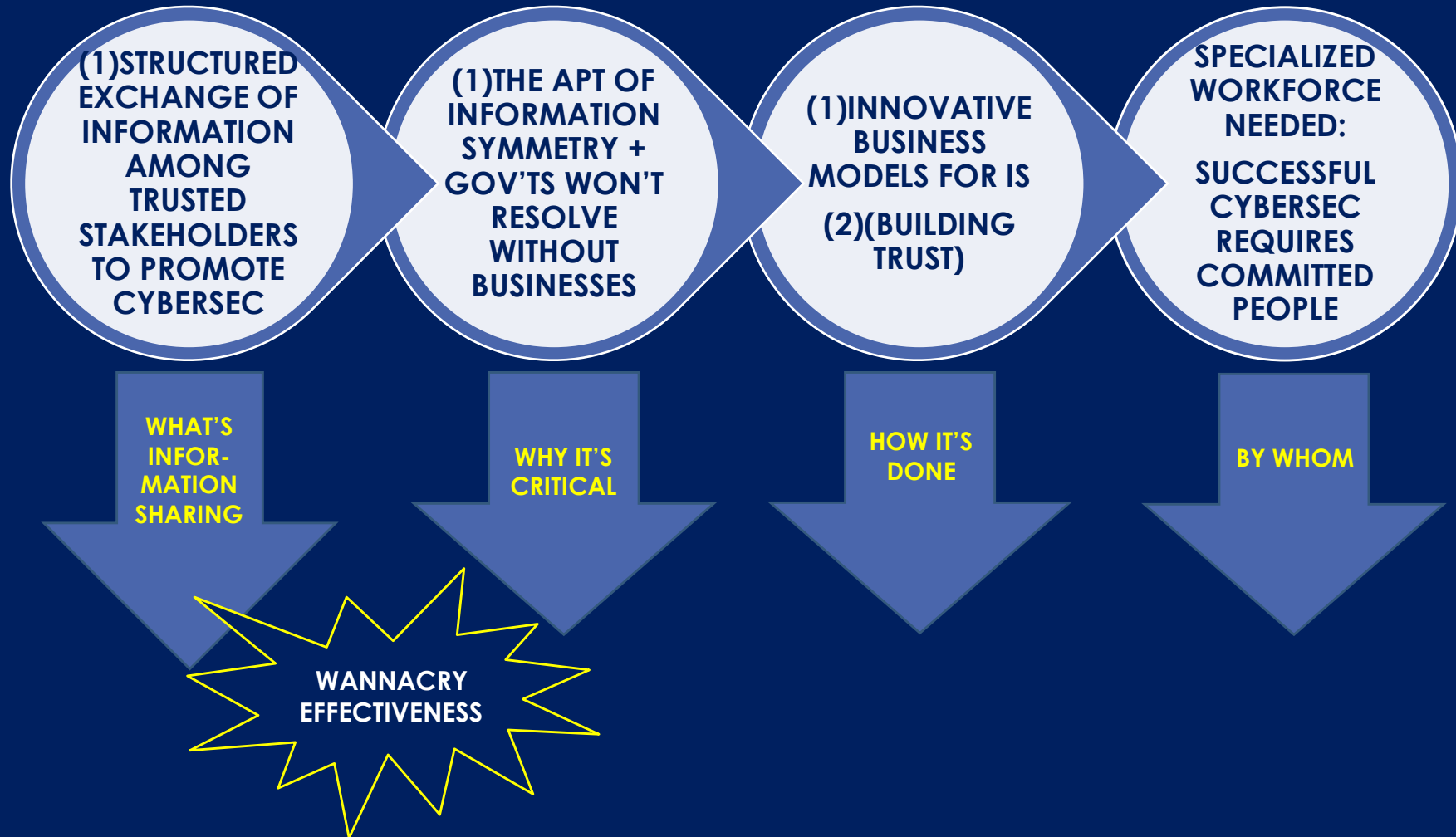
SOURCES: 1. 2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015. 2. ISACA 2015 APT Study, October 2015. 3. ISACA 2015 APT Study, October 2015. 4. The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, Juniper Research, May 2015. 5. SACA 2015 IT Risk/Reward Barometer-Member Study, 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. 9. State of Cybersecurity: Implications for 2015. 10. State of Cybersecurity: Implications for 2015. 11. Securing Our Future: Closing the Cybersecurity Skills 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.





WRAPPING UP



3 TAKEAWAYS

Information sharing in the financial sector is **evolving in innovative ways**, together with IS in other sectors



Trusted sharing platforms are critical, tailored to sectoral needs



Cybersecurity workforce development is also key – IS will not develop without it

BOTTOM LINE: REDUCING BARRIERS, ESTABLISHING TRUST



THE FEDERMANN
CYBER SECURITY CENTER
Cyber Law Program



האוניברסיטה העברית בירושלים
THE HEBREW UNIVERSITY OF JERUSALEM

The Federmann Cyber Security Center – Cyber Law Program

Home

About ▾

People ▾

The Clinic ▾

Research ▾

Deborah Housen-Couriel

Advisory Board



Deborah teaches international and Israeli cyber law at the Federmann Cyber Security Center, as well as at the Harvard Kennedy School's Exec Ed Program. She is a member of the committee that drafted the Tallinn 2.0 Manual on state activity in cyberspace. She is also a member of the Global Terrorism and International Law. Her current work at the Global Forum on Cyber Expertise and participation as a co-chair of the International Law Commission's Military Uses of Outer Space (MILAMOS) project. In 2010-2011, she served on the Regulatory Committee, under the aegis of the Prime Minister's Office. She is also a member of Israel's National Cyber Bureau's Public Committee on the Regulation of Cybersecurity. Her research focuses on global and Israeli cybersecurity law and regulation.

THANKS - ANY
QUESTIONS?