CSX™
CYBERSECURITY NEXUS

CYBERSECURITY NEXUS

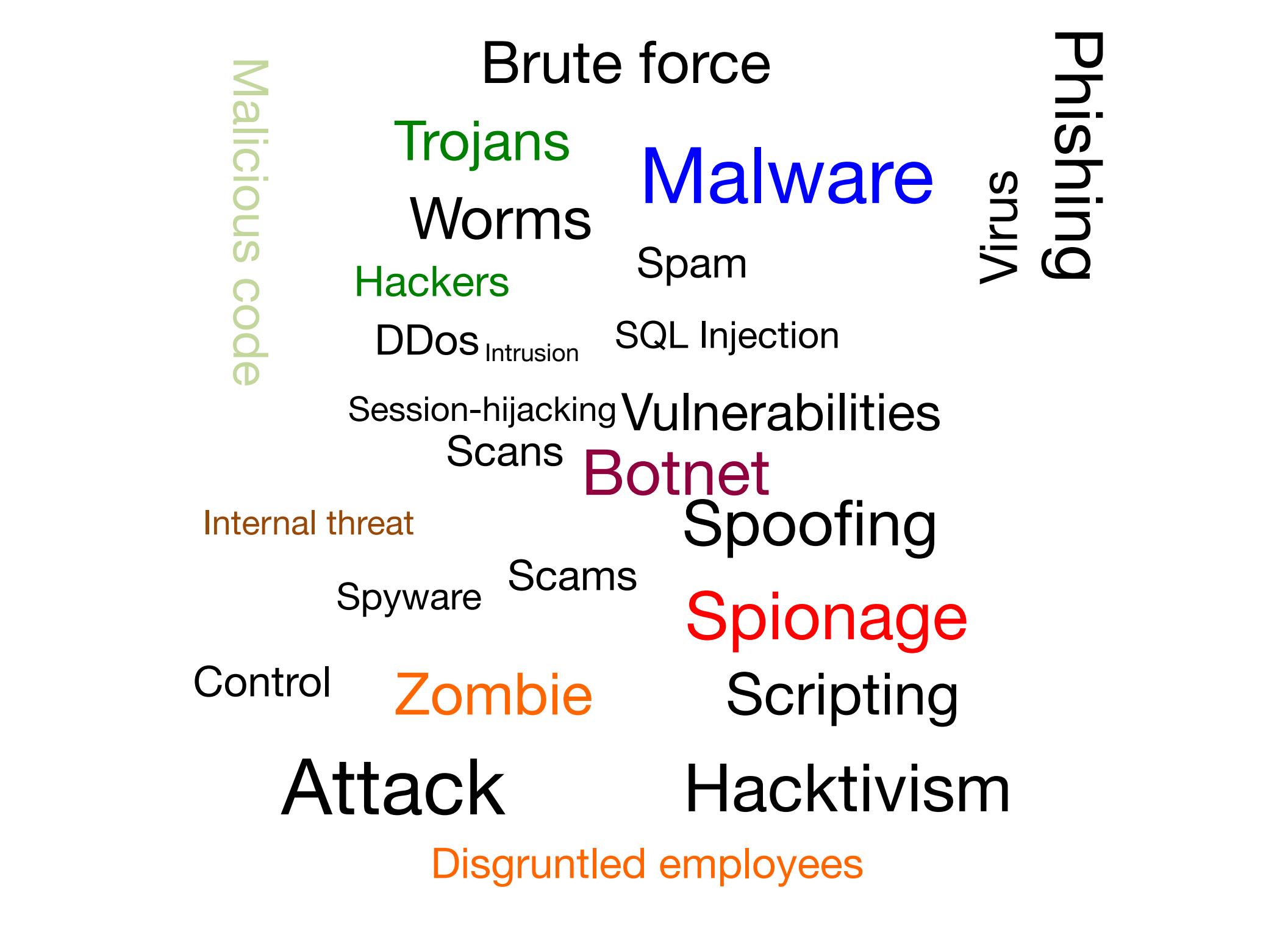
ROBERT E STROUD INTERNATIONAL PRESIDENT, ISACA

RAMSÉS GALLEGO INTERNATIONAL VICE PRESIDENT, ISACA

ISACA®
Trust in, and value from, information systems

Robert Stroud
International President, ISACA
VP Strategy & Innovation, CA Technologies
@RobertEStroud
RobertEStroud@live.com

Ramsés Gallego
CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT(f), Six Sigma Black Belt
International Vice President, ISACA
Security Strategist & Evangelist, Dell Software
Presidente, ISACA, Capítulo Barcelona
Privacy by Design Ambassador, Gobierno de Ontario, Canada
@ramsesgallego
ramses.gallego@me.com


Brute force
Malicious code
Trojans
Malware
Phishing
Worms
Virus
Spam
Hackers
DDos
Intrusion
SQL Injection
Session-hijacking
Vulnerabilities
Scans
Botnet
Internal threat
Spoofing
Scams
Spyware
Spionage
Control
Zombie
Scripting
Attack
Hacktivism
Disgruntled employees

US utility's control systems hit by advanced cyber attack - DHS

Published time: May 21, 2014 03:12 Get short URL

Reuters / Thomas Peter

472 183 2

An advanced group of hackers recently attacked a US public utility, compromising its control system network without affecting the utility's operations, according to the US Department of Homeland Security.

Tags
Crime, DHS, Hacking, Security, USA

The Department of Homeland Security (DHS) did not name the utility in a report released this week by the agency's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

"While unauthorized access was identified, ICS-CERT was able to work with the affected entity to put in place mitigation strategies and ensure the security of their control systems before there was any impact to operations," a DHS official told Reuters.

Source: http://rt.com/usa/160328-utility-cyber-attack-hack

ECB hacked: Data stolen from central bank

Matt Clinch | @mattclinch81
Thursday, 24 Jul 2014 | 5:25 AM ET

CNBC

Email addresses and other contact information stored at the **European Central Bank (ECB)** have been stolen, the organization confirmed on Thursday.

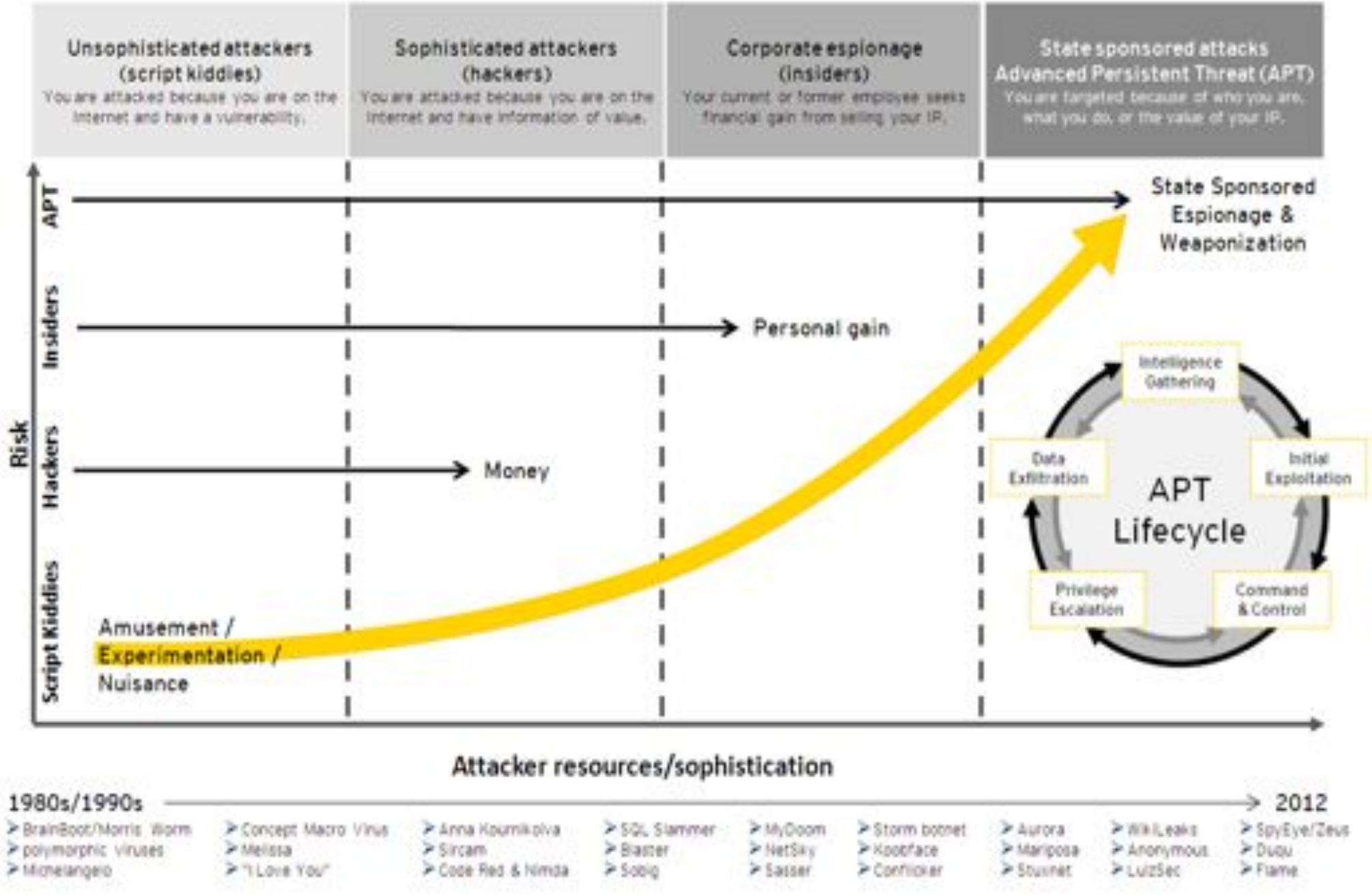
Security that protects a database serving its public website has been breached, it said in a statement published on its website, meaning users registering for information on conferences and visits at the ECB have been compromised.

Read More › Euro zone business activity rebounds, France lags

It stated that no "internal systems or market-sensitive" information had been part of the data theft and was physically separate from the compromised data.

Source: http://www.cnbc.com/id/101862753

EVOLUTION OF ATTACKS



Cybersecurity Skills Crisis

Too Many Threats

62% INCREASE IN BREACHES **IN 2013**[1]

1 IN 5 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[4]

US **$3 TRILLION** TOTAL GLOBAL IMPACT OF **CYBERCRIME**[3]

7½ MONTHS IS THE *AVERAGE* TIME **AN ADVANCED THREAT GOES UNNOTICED** ON VICTIM'S NETWORK[2]

2.5 BILLION **EXPOSED RECORDS** AS A RESULT OF A DATA BREACH IN THE PAST 5 YEARS[5]

Too Few Professionals

62% OF ORGANIZATIONS **HAVE NOT INCREASED SECURITY TRAINING IN 2014**[6]

1 OUT OF 3 SECURITY PROS ARE **NOT FAMILIAR WITH ADVANCED PERSISTENT THREATS**[7]

<2.4% GRADUATING STUDENTS **HOLD COMPUTER SCIENCE DEGREES**[8]

1 MILLION UNFILLED SECURITY JOBS WORLDWIDE[9]

83% **OF ENTERPRISES** CURRENTLY LACK THE RIGHT SKILLS AND HUMAN RESOURCES TO PROTECT THEIR IT ASSETS[10]

Enterprises are under siege from **a rising volume of cyberattacks.**

At the same time, the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed, organizations will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry-level practitioners to seasoned professionals.

SOURCES: 1. *2014 Internet Security Threat Report, Volume 19*, Symantec, April 2014; **2.** *M-Trends 2014: Attack the Security Gap*, Mandiant, April 2014; **3.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **4.** *ISACA's 2014 APT Study*, ISACA, April 2014; **5.** *An Executive's Guide to 2013 Data Breach Trends*, Risk Based Security/Open Security Foundation, February 2014; **6.** *ISACA's 2014 APT Study*, ISACA, April 2014; **7.** *ISACA's 2014 APT Study*, ISACA, April 2014; **8.** Code.org, February 2014; **9.** *2014 Cisco Annual Security Report*, Cisco, January 2014; **10.** *Cybersecurity Skills Haves and Have Nots*, ESG, March 2014

CSX

ISACA

CSX ELEMENTS

AVAILABLE NOW

- Cybersecurity Fundamentals Certificate (workshops and exams taking place in Q3; first workshop sold out)
- *Transforming Cybersecurity Using COBIT 5*
- *Responding to Targeted Cyberattacks*
- *Advanced Persistent Threats: Managing the Risks to Your Business*
- 2014 APT Awareness Study
- Cybersecurity webinars and conference tracks (six-part webinar series)
- Cybersecurity Knowledge Center community
- Implementation guidance for NIST's US Cybersecurity Framework (which incorporates COBIT 5) and the EU Cybersecurity Strategy

COMING SOON

- Mentoring Program
- Cybersecurity practitioner-level certification (first exam: 2015)
- Cybersecurity training courses
- SCADA guidance
- Digital forensics guidance

. . . . And announcing

CAREER PATH

0-3 years:	**Cybersecurity Fundamentals Certificate** (no experience required; must pass knowledge-based exam)
3-5 years:	**Cybersecurity practitioner-level certification** (coming in mid-2015)
5+ years:	**Certified Information Security Manager certification** (25,000+ professionals certified since inception)

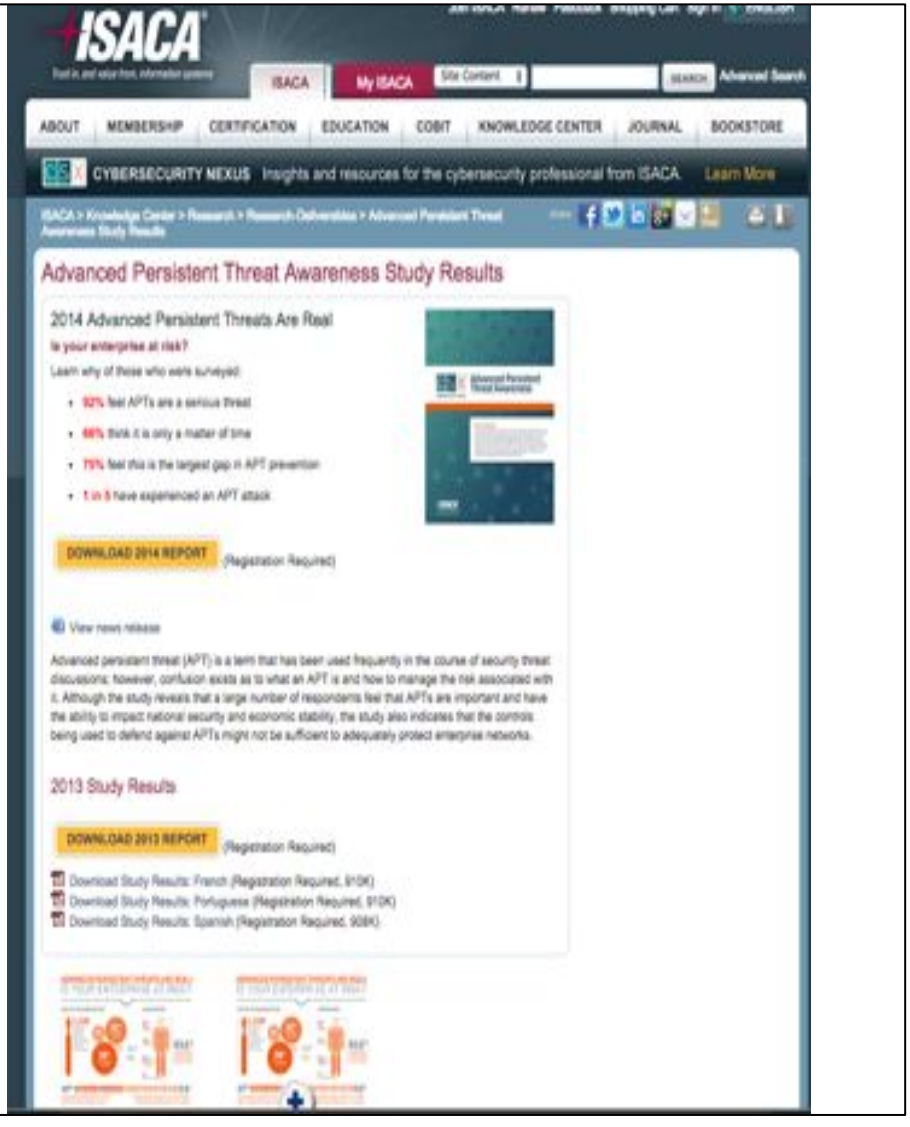
CYBERSECURITY FUNDAMENTALS KNOWLEDGE CERTIFICATE

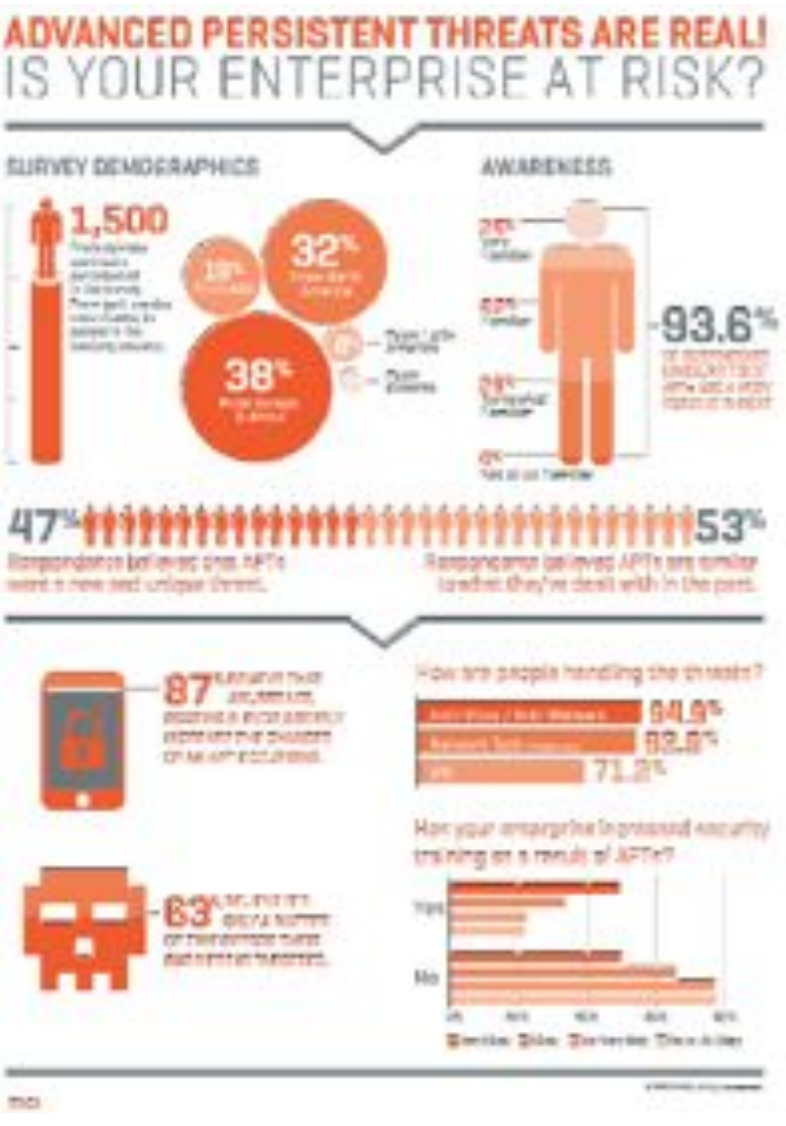
- Knowledge-based exam for those with 0 to 3 years experience

- Foundational level covers four domains:
  1) Cybersecurity architecture principles
  2) Security of networks, systems, applications and data
  3) Incident response
  4) Security implications related to adoption of emerging technologies

The content aligns with the US NICE framework and was developed by a team of about 20 cybersecurity professionals from around the world. The team is involved in all areas of development through content contribution and subject matter expert reviews.

ADVANCED PERSISTENT THREAT AWARENESS STUDY

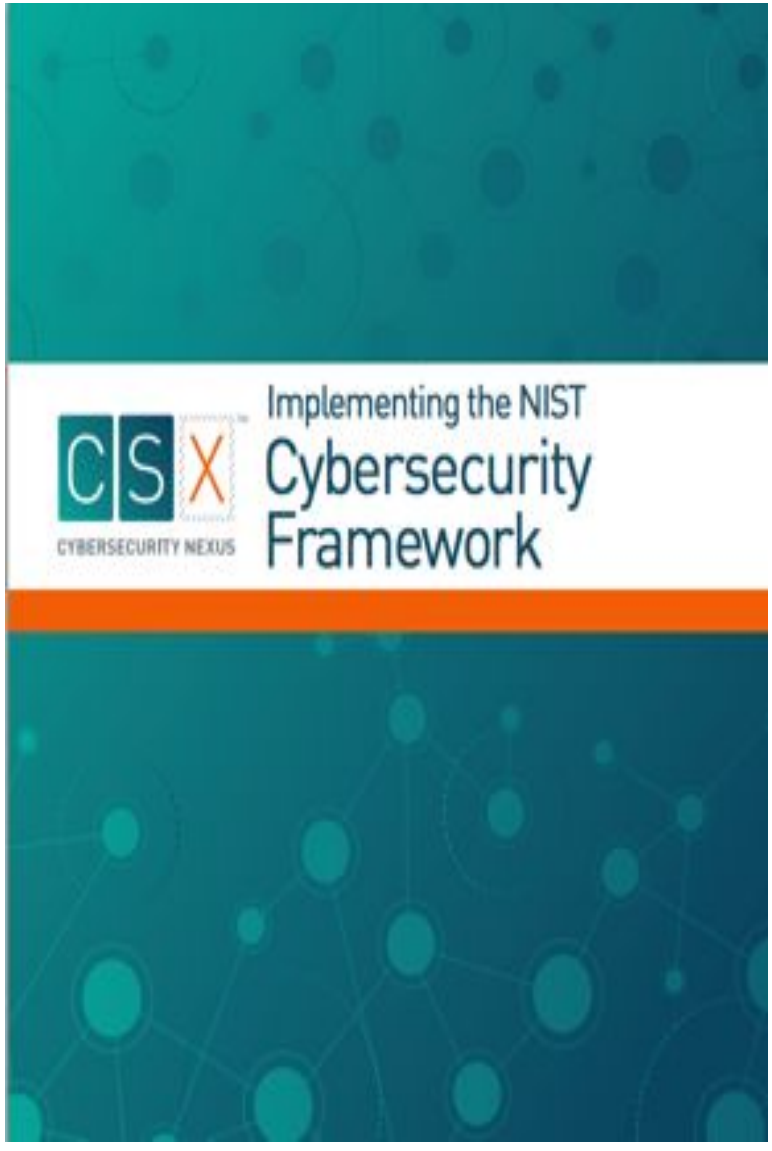




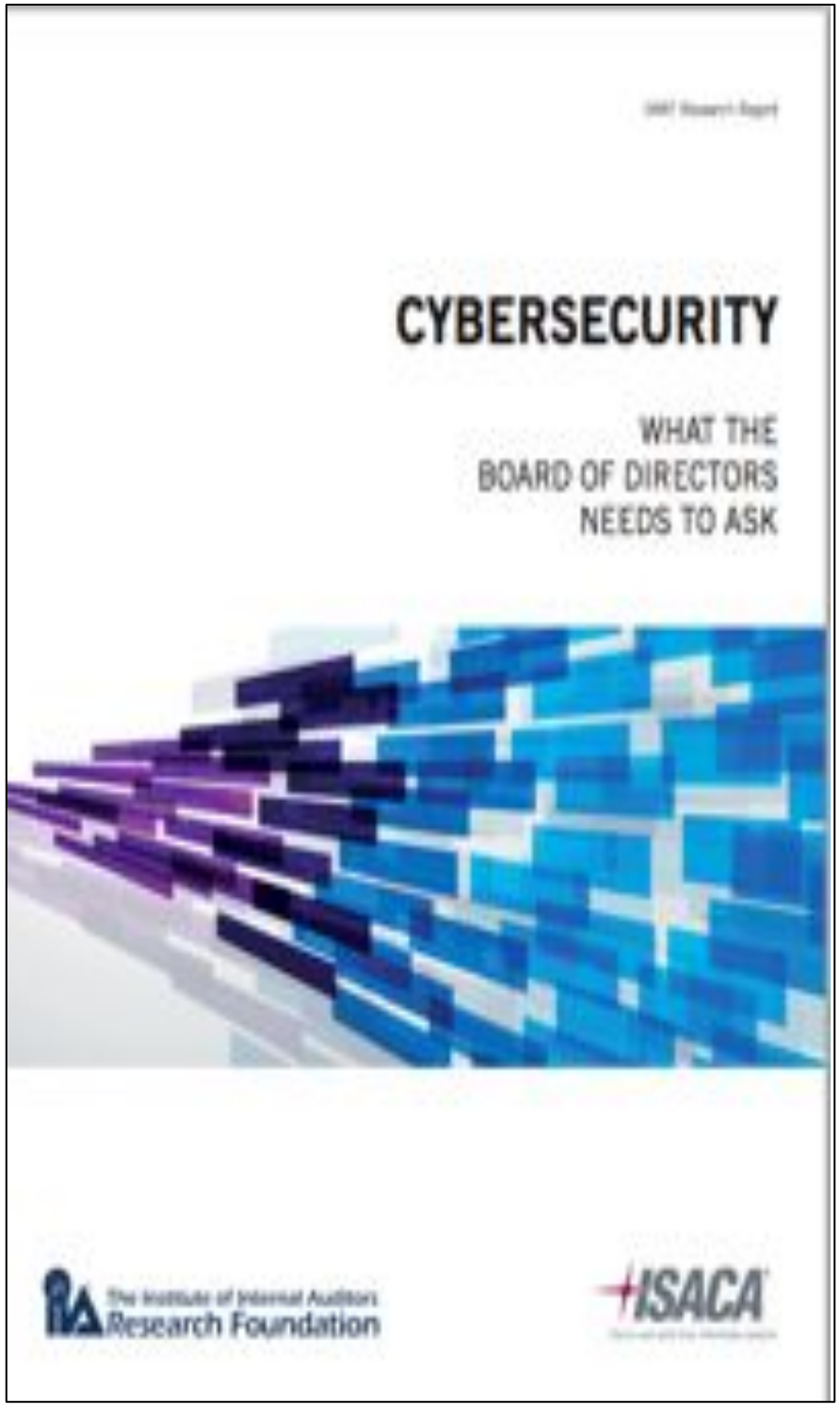
CSX EUROPEAN GUIDANCE

- **European Cybersecurity Implementation Series:**
  - *European Cybersecurity Implementation: Overview*
  - *European Cybersecurity Implementation: Assurance*
  - *European Cybersecurity Implementation: Resilience*
  - *European Cybersecurity Implementation: Risk Guidance*
  - www.isaca.org/EU-cyber-implementation

SPECIFIC GUIDANCE FOR THE NIST FRAMEWORK



LEADERSHIP FOR EXECUTIVES WITH THE IIA



TRANSFORMING CYBERSECURITY USING COBIT 5

Eight Key Principles:

1. Understand the potential impact of cybercrime and warfare on your enterprise.
2. Understand end users, their cultural values and their behavior patterns.
3. Clearly state the business case for cybersecurity and the risk appetite of the enterprise.
4. Establish cybersecurity governance.
5. Manage cybersecurity using principles and enablers. (The principles and enablers found in COBIT 5 will help your organization ensure end-to-end governance that meets stakeholder needs, covers the enterprise to end and provides a holistic approach, among other benefits. The processes, controls, activities and key performance indicators associated with each enabler will provide the enterprise with a comprehensive picture of cybersecurity.)
6. Know the cybersecurity assurance universe and objectives.
7. Provide reasonable assurance over cybersecurity. (This includes monitoring, internal reviews, audits and, as needed, investigative and forensic analysis.)
8. Establish and evolve systemic cybersecurity.

AND ANNOUNCING . . .

“Becoming a successful security practitioner is hard. Ideal candidates are well-rounded and have a solid foundation in networking, operating systems, web technologies and incident response, and an understanding of the threat landscape and risk management.”

Darren Van Booven, CISA, CISM, CISSP, CPA, Chief Information Security Officer, U.S. House of Representatives, and ISACA Member

CSX™
CYBERSECURITY NEXUS

www.isaca.org/cyber

ISACA®
Trust in, and value from, information systems

CSX™
CYBERSECURITY NEXUS

THANK YOU

For more information: https://www.isaca.org

ISACA®
Trust in, and value from, information systems