(ISC)²®

INSPIRING A SAFE AND SECURE CYBER WORLD.

Defending Against Cybersecurity Threats from Using Big Data

Security World 2016

Hanoi, Vietnam

Philip Victor

pvictor@isc2.org

Head of Market Development, Asia-Pacific

(ISC)^2

Big Data

- Big data & data warehousing are techniques of amassing huge amounts of data
- Data may be bridged across a number of storage locations
- ***"Big data is the frontier of a firm's ability to store, process, and access all the data it needs to operate effectively, make decisions, reduce risks, and serve customers."*** – Mike Gualtieri, Forrester

Security Concerns

- Database structures
- Scalability
- Configuration management
- Cost
- Operations

Database Structures

- Although most traditional database vendors support big data, they operate as SQL-based or another type of relational structure.
- Hadoop (open source project for big data) and other next-generation databases are designed for unstructured data

Scalability

- Most structured database systems are designed to "scale up" based on the size of the host machine, next-generation technologies are often designed to "scale out," or cluster
- Instead of having a single large database server, an agency may have 500 smaller systems operating together as a cluster. Some of these systems could be virtual, some physical, and some in the cloud.

Configuration Management

- Traditionally, FISMA (through FIPS-200) has required agencies to develop robust configuration management plans, develop configuration and change management boards, and ensure that security impact analysis is performed as part of system changes
- With big data, mature and robust configuration and change management is a must.

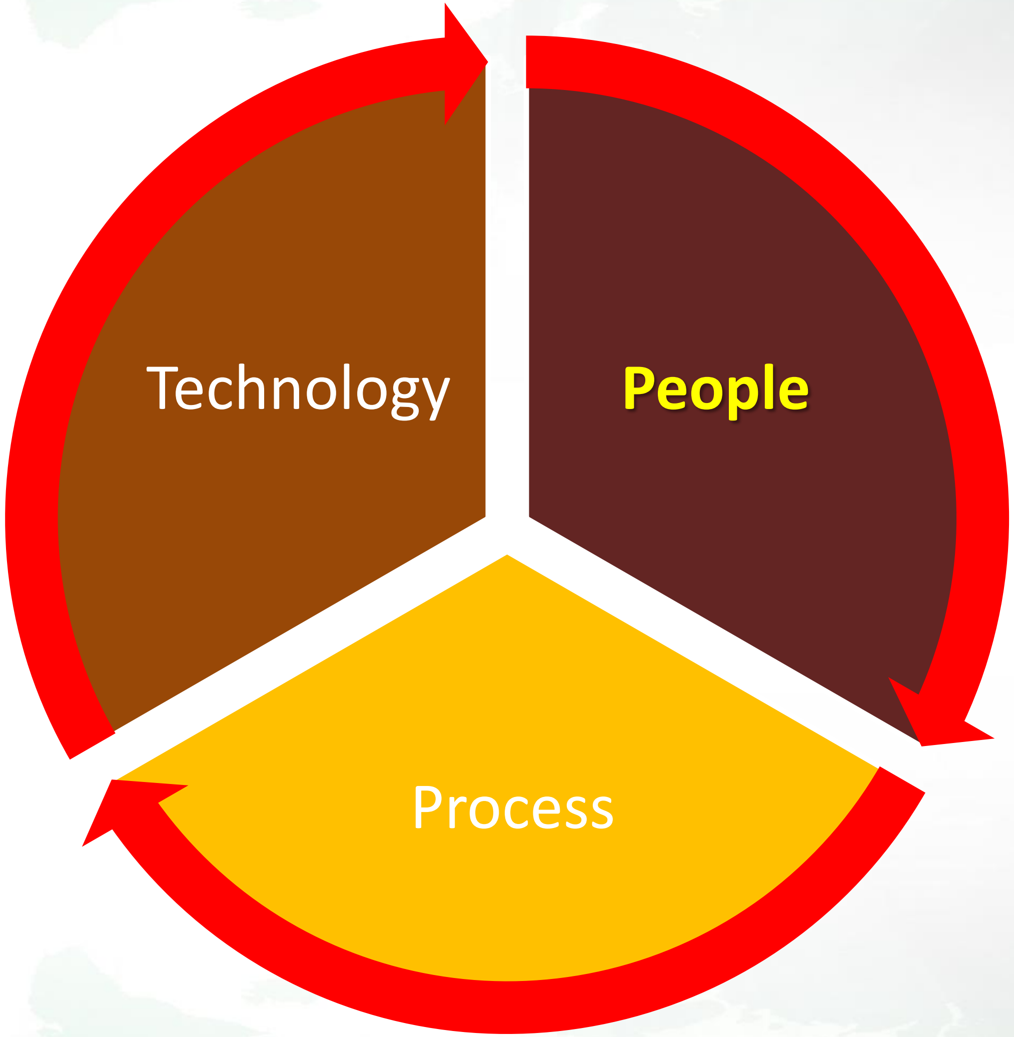
Cost

- Since new nodes could be spun up in almost any cloud provider's environment, or even on additional desktops within an agency, tight control over IT resources and spending must be in place

Operations

- Who is responsible for patching? Who is responsible for vulnerability scanning? What happens if the software has a vulnerability and there is no vendor to contact for support?
- Many big data platforms are capable of utilizing cloud services out of the box, the security team must be aware of any changes being performed as part of the system lifecycle
- Security teams must look at big data from a holistic perspective of protecting the infrastructure and operating system, applying as much automation and existing policy as possible.

Addressing the Issues



Addressing the Issues

- Big Data is more about the processing techniques and outputs than the size of the data set itself, so *specific skills* are required to use Big Data effectively
- There is a general shortage of *specialist skills* for Big Data analysis, in particular when it comes to using some of the less mature technologies.

Workforce Development

- People & skills are critical and vital
- Having the *right people* and skill sets that form a specialized team is a critical success factor for Big Data deployment
- As big data is “scale-up”, various skills are needed and certified professionals in various areas are crucial.

Right Skills Set?

- The need to ask the questions for specific operations and functions
- Knowing how to use big data for business transformation
- The main factor: Having qualified and certified professionals who knows how to view security from a holistic point of view and have a solid security strategy to prevent and defend against cyber attacks and threats

About (ISC)²®

- Established in 1989 – Non-profit consortium of information security industry
- Global leaders in certifying and educating information security professionals throughout their careers
- Global standard for information security – (ISC)² CBK®, a compendium of information security topics
- Over 110,000 certified professionals in more than 160 countries
- Over 14,000 certified professionals in Asia Pacific

Mission and Vision

Mission: Support and provide members with credentials, resources, and leadership to secure information and deliver value to society

Vision: Inspiring a safe and secure cyber world

What does (ISC)$^{2®}$ do?

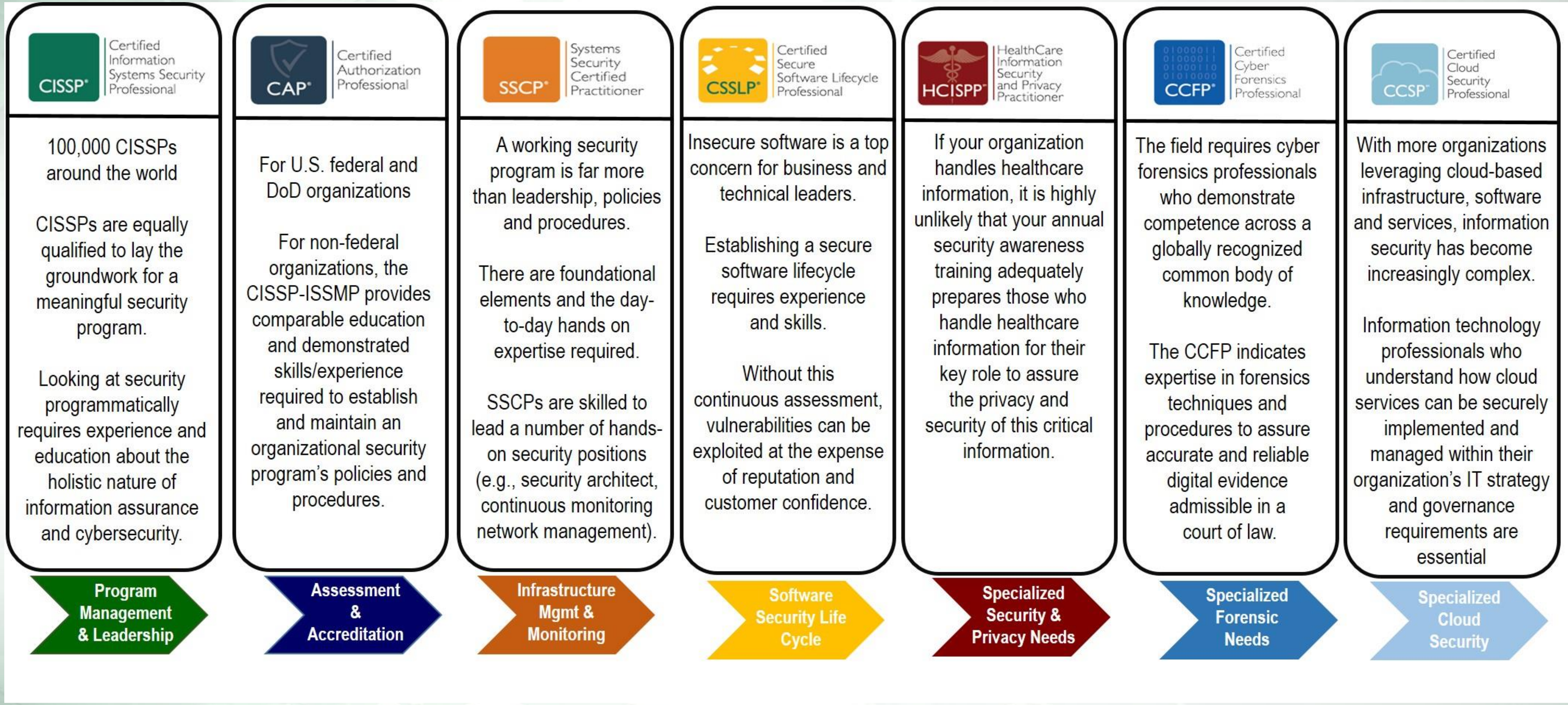
(ISC)^2 is the developer of a collection of ANSI/ISO/IEC 17024 certifications for information security professionals worldwide.

(ISC)^2 developed a new certification particularly for those stakeholders within the network monitoring and investigation space - Forensics.

(ISC)^2 provides a wide array of educational programs, taught around the world, in classrooms and online

(ISC)^2 membership is exclusive to those professionals with (ISC)^2 certifications

(ISC)^2 Credentials



CISSP® Certified Information Systems Security Professional

100,000 CISSPs around the world

CISSPs are equally qualified to lay the groundwork for a meaningful security program.

Looking at security programmatically requires experience and education about the holistic nature of information assurance and cybersecurity.

Program Management & Leadership

CAP® Certified Authorization Professional

For U.S. federal and DoD organizations

For non-federal organizations, the CISSP-ISSMP provides comparable education and demonstrated skills/experience required to establish and maintain an organizational security program's policies and procedures.

Assessment & Accreditation

SSCP® Systems Security Certified Practitioner

A working security program is far more than leadership, policies and procedures.

There are foundational elements and the day-to-day hands on expertise required.

SSCPs are skilled to lead a number of hands-on security positions (e.g., security architect, continuous monitoring network management).

Infrastructure Mgmt & Monitoring

CSSLP® Certified Secure Software Lifecycle Professional

Insecure software is a top concern for business and technical leaders.

Establishing a secure software lifecycle requires experience and skills.

Without this continuous assessment, vulnerabilities can be exploited at the expense of reputation and customer confidence.

Software Security Life Cycle

HCISPP® HealthCare Information Security and Privacy Practitioner

If your organization handles healthcare information, it is highly unlikely that your annual security awareness training adequately prepares those who handle healthcare information for their key role to assure the privacy and security of this critical information.

Specialized Security & Privacy Needs

CCFP® Certified Cyber Forensics Professional

The field requires cyber forensics professionals who demonstrate competence across a globally recognized common body of knowledge.

The CCFP indicates expertise in forensics techniques and procedures to assure accurate and reliable digital evidence admissible in a court of law.

Specialized Forensic Needs

CCSP℠ Certified Cloud Security Professional

With more organizations leveraging cloud-based infrastructure, software and services, information security has become increasingly complex.

Information technology professionals who understand how cloud services can be securely implemented and managed within their organization's IT strategy and governance requirements are essential

Specialized Cloud Security

Summary

- Big data is complex and requires analytical capabilities for success
- The key differentiating factor is the human factor
- A successful organization have the right skills and expertise with a qualified workforce to make big data a success.

(ISC)²®

CISSP® ISSAP® ISSEP® ISSMP® SSCP® CAP® CSSLP® CCFP® HCISPP℠ CCSP℠

INSPIRING A SAFE AND SECURE CYBER WORLD.