WeLCOme

Kent King – CISSP, CISA, CISM, CRISC, SSCP

Email: kking83@cscc.org

What does the term "Security" mean to you?

" FOR A MOMENT, I HAD A FEELING OF TOTAL SECURITY. THEN IT WENT AWAY. "

Security for Businesses

Security must be measurable

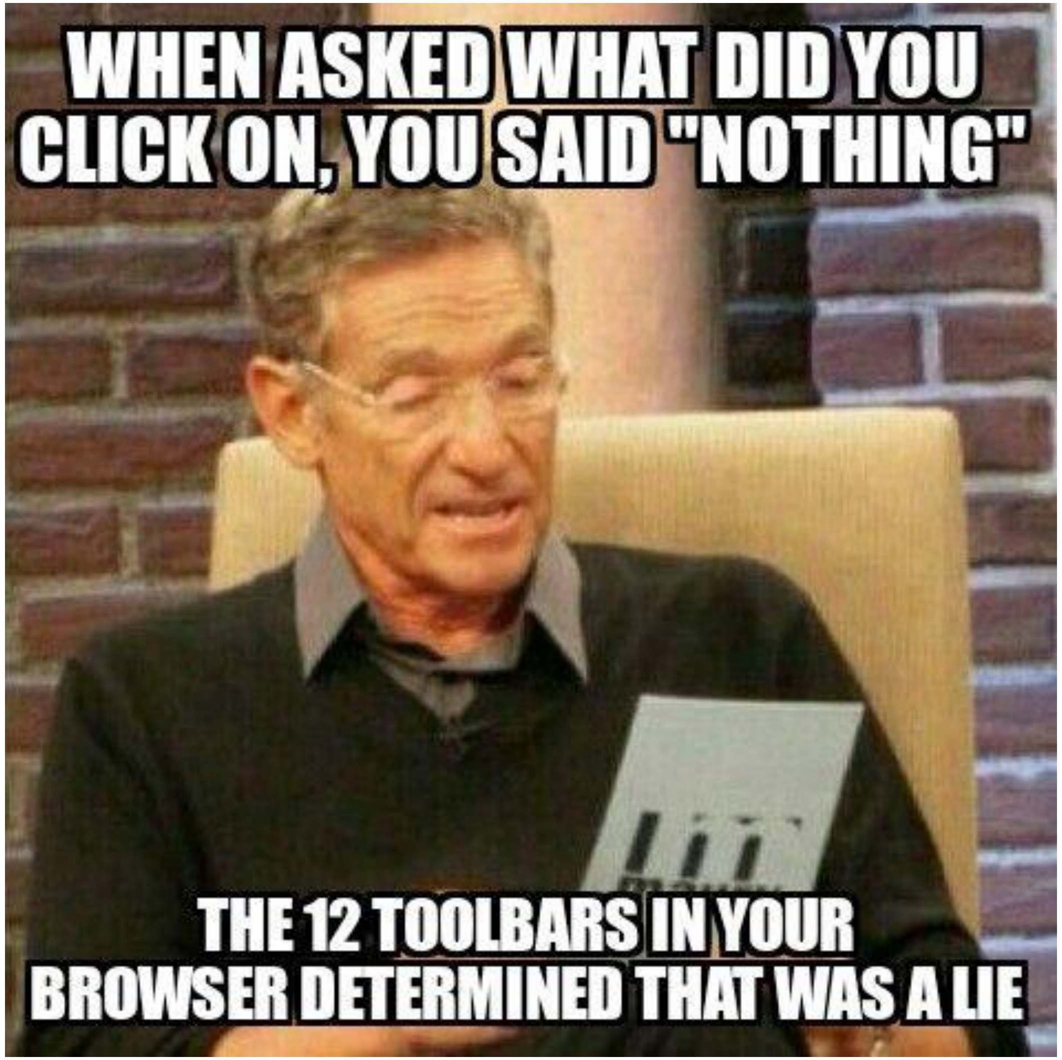
Security must be based on business objectives

Challenges

- The information security strategy must be aligned with the strategic direction of the organization.
- It must be integrated into business processes.
- Security programs will always be affected by a lack of support and inadequate budgets.
- There simply is not enough time to do everything that needs to be done.
- The battle only escalates.

Objectives

- Give you a foundational knowledge of cybersecurity
- Learn the terminology
- Apply core principles in real-world situations
- Give you enough background to initiate your cybersecurity career


WHEN ASKED WHAT DID YOU CLICK ON, YOU SAID "NOTHING"
THE 12 TOOLBARS IN YOUR BROWSER DETERMINED THAT WAS A LIE

Security Frameworks

- ISO 27001/27002
- COBIT - ISACA
- ITIL - IT Service delivery best practices
- Risk Management Framework (NIST 800 series)

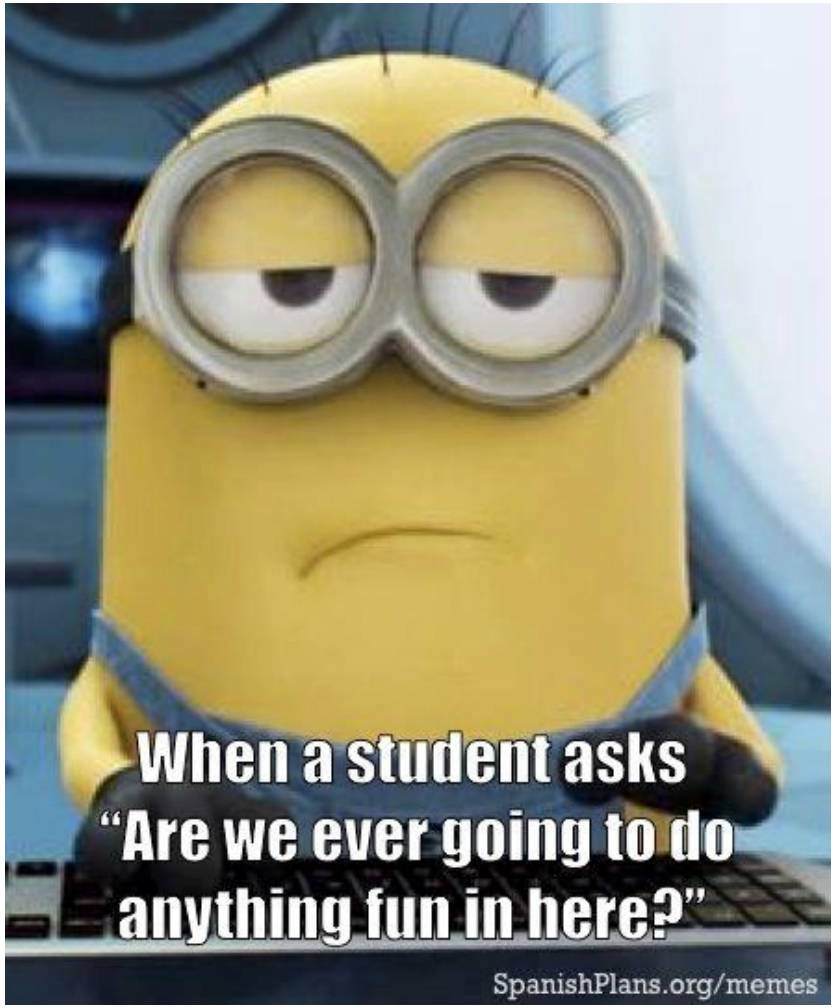
Security Blogs

- https://krebsonsecurity.com/
- https://threatpost.com/
- https://www.csoonline.com/
- https://isc.sans.edu/
- https://www.darkreading.com/
- https://www.schneier.com/
- https://thehackernews.com/
- https://blog.erratasec.com/
- https://securityboulevard.com/
- https://www.grahamcluley.com/

Also visit product vendors, especially antivirus/antimalware companies.

Classroom Time

- Review online materials
- Review quiz results
- Review assignments
- Discuss real-world applications
- Introduce the next domain



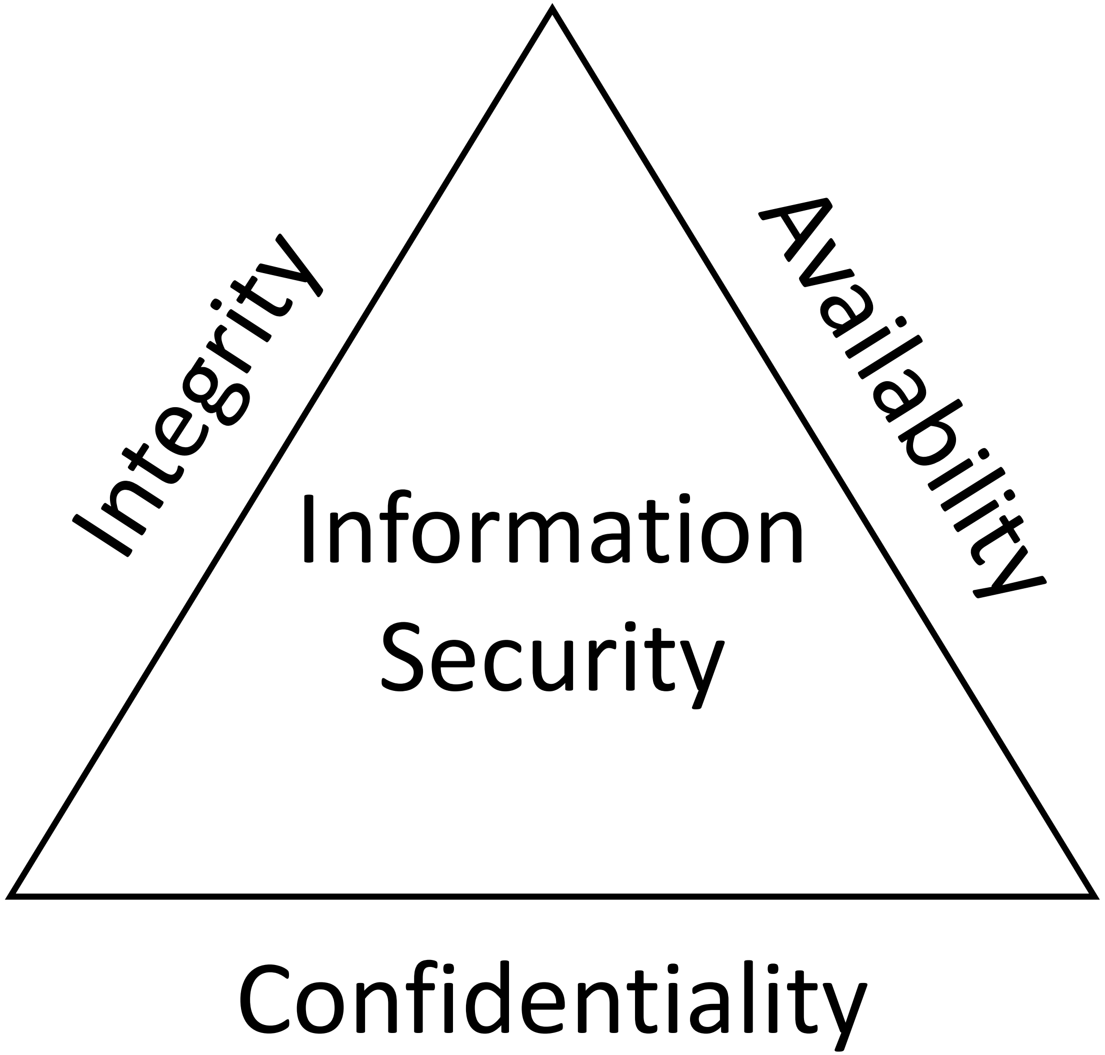
Time for
a BREAK

Systems Security Certified Practitioner

ISC² - The International Information System Security Certification Consortium

Systems Security Certified Practitioner (SSCP)

- Access Controls
- Security Operations and Administration
- Risk Identification, Monitoring, and Analysis
- Incident Response, and Recovery
- Networks and Communications Security
- Cryptography
- Systems and Applications Security


Integrity
Availability
Information Security
Confidentiality

Confidentiality

The property of information in which it is only made available to those who have a legitimate need to know

Each level of confidentiality is associated with a particular protection class

Consequences of a Breach

Legal and regulatory fines and sanctions

Loss of customer and investor confidence

Loss of competitive advantage

Civil litigation

Integrity

The property of information whereby it is recorded, used, and maintained in a way that ensures its completeness, accuracy, internal consistency, and usefulness for a stated purpose

Consequences of Integrity Failure

Inability to read or access critical files

Errors

Failures in information processing

Calculation errors

Uninformed decision making by business leaders

Availability

access
when and
as needed

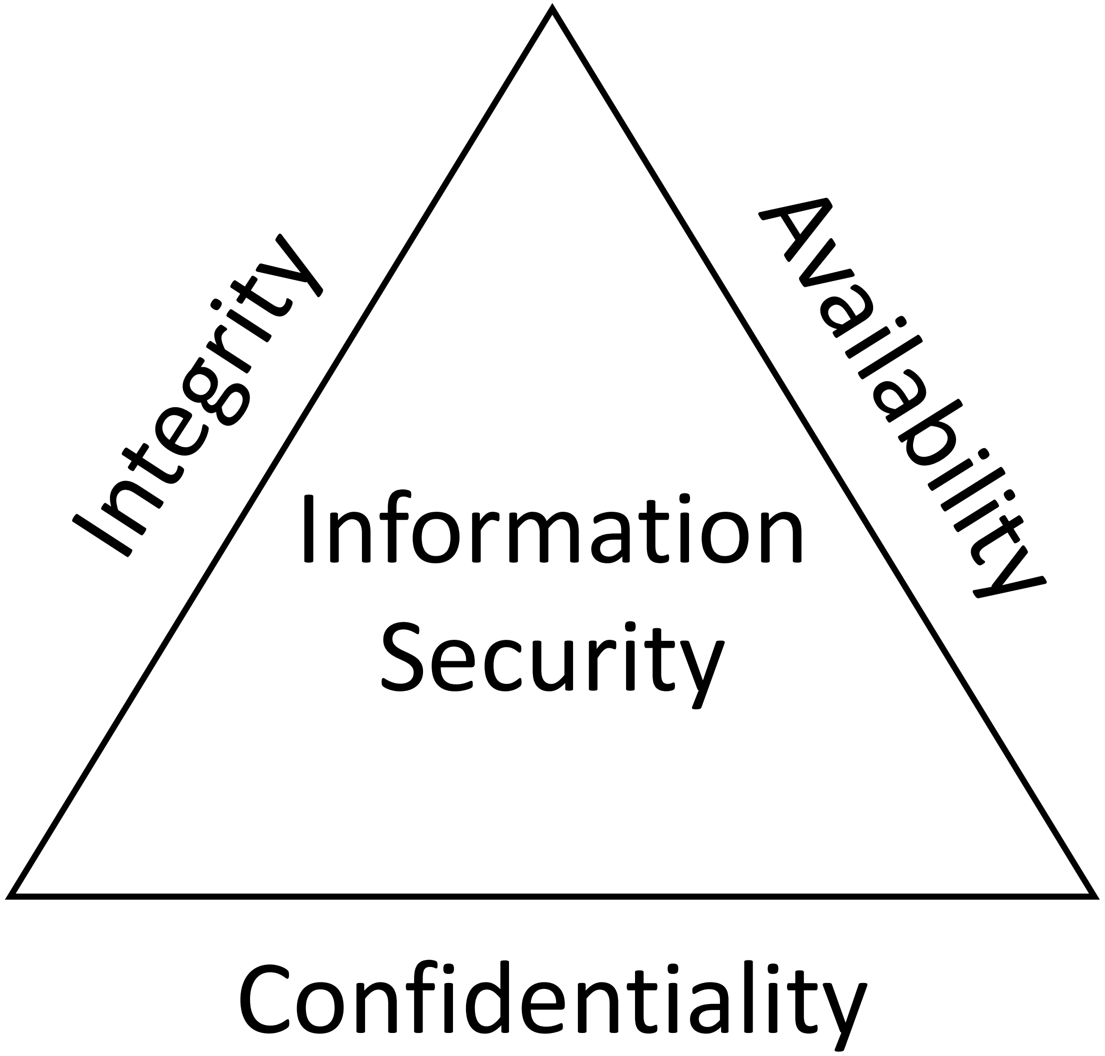
The ability to access and use information systems when and as needed to support an organization's operations

Consequences of Availability Failures

1 **Interruption in services and revenue streams**

2 **Fines and sanctions**

3 **Errors in transaction processing and decision making**


Integrity
Availability
Information Security
Confidentiality

OTHERS

Non-Repudiation

A service that ensures that the sender cannot deny a message was sent and the integrity of the message is intact

Privacy

collection,
use, retention,
and disclosure
of P.I

The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information

Least Privilege

access based on the need of the user or process.

Access rights are permissions granted based on the need of a user or process to access and use information and resource

Systems Security Certified Practitioner

SSCP

(ISC)²

Least Privilege and COTS Applications

COTS- Commercial Off The Self

Many COTS applications are developed in environments that have not adopted least privilege principles and, as a result, these products often require elevated privilege to run

Separation of Duties

Separation of duties

✓ Requires two or more individuals to complete a task or perform a specific function

Dual control

✓ Requires two or more people operating at the same time to perform a single function

Defense-in-Depth

Defenses may be designed to prevent or deter attack using an outside-in or inside-out approach

By placing safeguards at two or more points along the access path to the asset, failure of one safeguard can be counteracted

Risk-Based Controls

RISK = THREAT + VULNERABILITY + IMPACT

Authorization and Accountability

A tie actions to users → LOGs

A record of authorizations should be kept to support access control system validation testing

Accountability is a principle that ties authorized users to their actions

Information Security - More than electronic data

- Keys
- Cell Phone
- Access Cards
- Logged-In Computer
- Printouts
- Passwords on Sticky Notes
- Open File Cabinet
- Personal Mail

Asset Categories

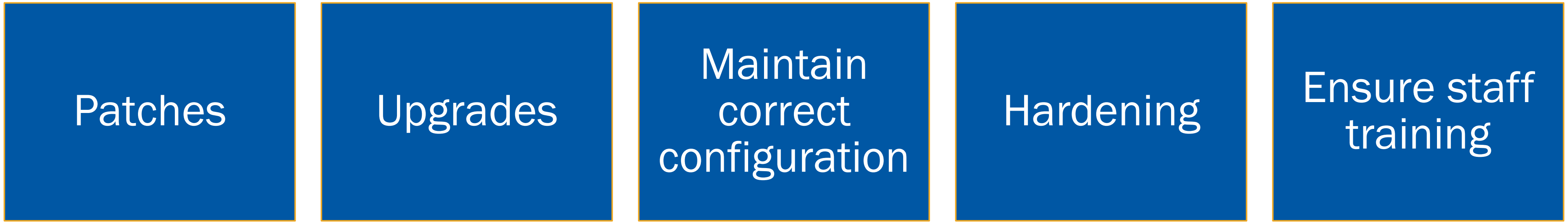
Primary Assets	Supporting Assets
Business processes and activities	Hardware
Information	Software
	Network
	Personnel
	Site
	Organization’s structure

Asset Protection

Each asset should be provided an appropriate level of protection.

Adequate or appropriate protection commensurate with risk.

Hardware Operations and Maintenance



Patches

Upgrades

Maintain correct configuration

Hardening

Ensure staff training

Software Management

- Build or Buy?
- Source code escrow
- Patching
- Documentation
- Licensing and Software Piracy

Information

- One of the most valuable assets of an organization
- Also one of the most vulnerable

Loss of information may lead to:

- Fines
- Reputational damage
- Business interruption
- Loss of competitive advantage

Information Classification

Classification ensures the appropriate level of protection for information.

Requires determination of information owner.

Information must be protected in all forms and at all times, in all places.

Third Party/Outsourcing Implications

- Cloud and other outsourcing options
- Legal liabilities for asset protection
- Contractual agreements
- Monitoring
- Disposal of equipment by outsourcing firm

During the week

- Review Unit 1 online course material
  - Understanding Security Concepts
  - Participate in Asset Management
- Complete the quiz