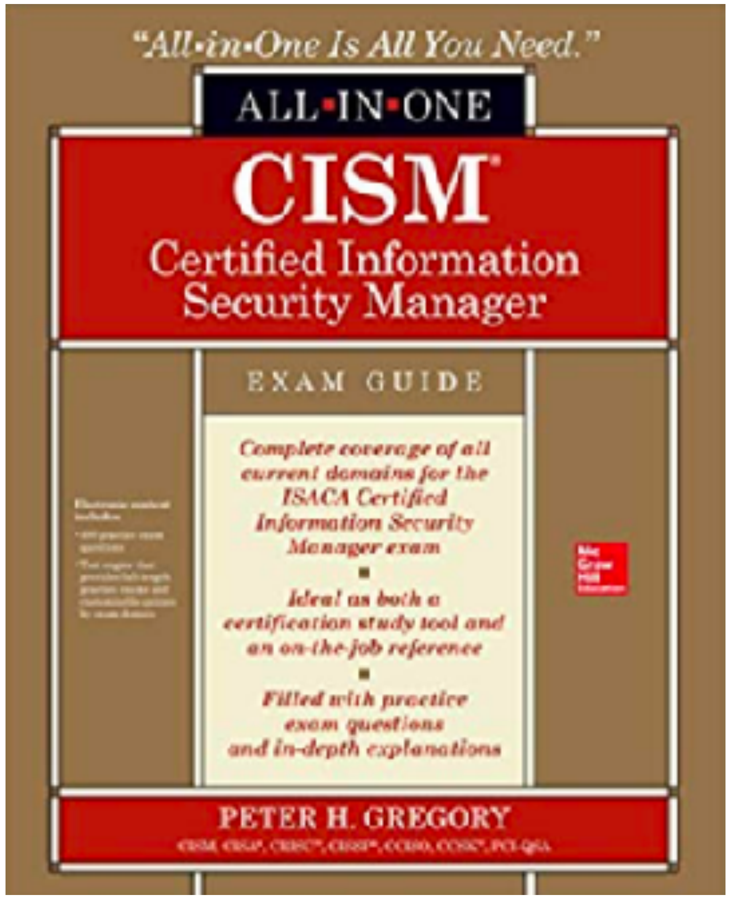
CNIT 160: Cybersecurity Responsibilities

4. Information Security Program Development Part 4

Pages 257-275


"All-in-One Is All You Need."
ALL-IN-ONE
CISM
Certified Information Security Manager
EXAM GUIDE
Complete coverage of all current domains for the ISACA Certified Information Security Manager exam
Ideal as both a certification study tool and an on-the-job reference
Filled with practice exam questions and in-depth explanations
PETER H. GREGORY

Topics in this Lecture

- **Administrative Activities**
  - **External Partnerships (p. 257)**
  - **Compliance Management**
  - **Personnel Management**
  - **Project and Program Management**
  - **Budget**
  - **Business Case Development**
  - **Vendor Management**
- **Security Program Operations**
  - **Event Monitoring**
  - **Vulnerability Management**

Chapter Topics For Later Lectures

- **Security Program Operations**
  - **Secure Engineering and Development**
  - **Network Protection (p. 277)**
  - **Endpoint Protection & Mgmt (p. 288)**
  - **Identity and Access Management (p. 292)**

Chapter Topics For Later Lectures

- **Security Program Operations**
  - **Security Incident Management**
  - **Security Awareness Training**
  - **Managed Security Services Providers**
  - **Data Security (p. 302)**
  - **Business Continuity Planning**

Chapter Topics
For Later Lectures

- **IT Service Management (p. 322)**
- **Controls**
- **Metrics and Monitoring**
- **Continuous Improvement**

Administrative Activities
External Partnerships

Law Enforcement

- Cultivate relationships in advance of incidents
- USA
  - FBI (InfraGard)
  - Secret Service (HTCIA)
- Global
  - Interpol

Regulators and Auditors

- **Partners, not adversaries**
- **Understand their ethical boundaries**

Standards Organizations

- **PCI Security Standards Council**
- **Cloud Security Alliance**
- **Information Security Forum**
- **International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)**

Professional Organizations

- **ISACA**
  - **Developer of CISM and CISA certifications**
- **ISSA (Information Systems Security Association)**
- **(ISC)^2 (International Information Systems Security Certification Consortium)**
  - **Developer of CISSP certification**

Professional Organizations

- **CSA (Cloud Security Alliance)**
- **EC-Council (International Council of Electronic Commerce Consultants)**
  - **Developer of CEH (Certified Ethical Hacker) certification**
- **SANS**
  - **Developer of GIAC certifications**

Security Professional Services Vendors

- **Essential partners of security managers**
- **Must develop trusted relationships**
- **Virtual CISOs or CISO advisors**
- **Can assist with strategy for**
    - **acquisition, implementation, and operation of security tools**

Security Product Vendors

- **Need good relationships with vendors**
- **Often an area with problems**
- **Constantly changing**
- **New vendors, new products**

Administrative Activities Compliance Management

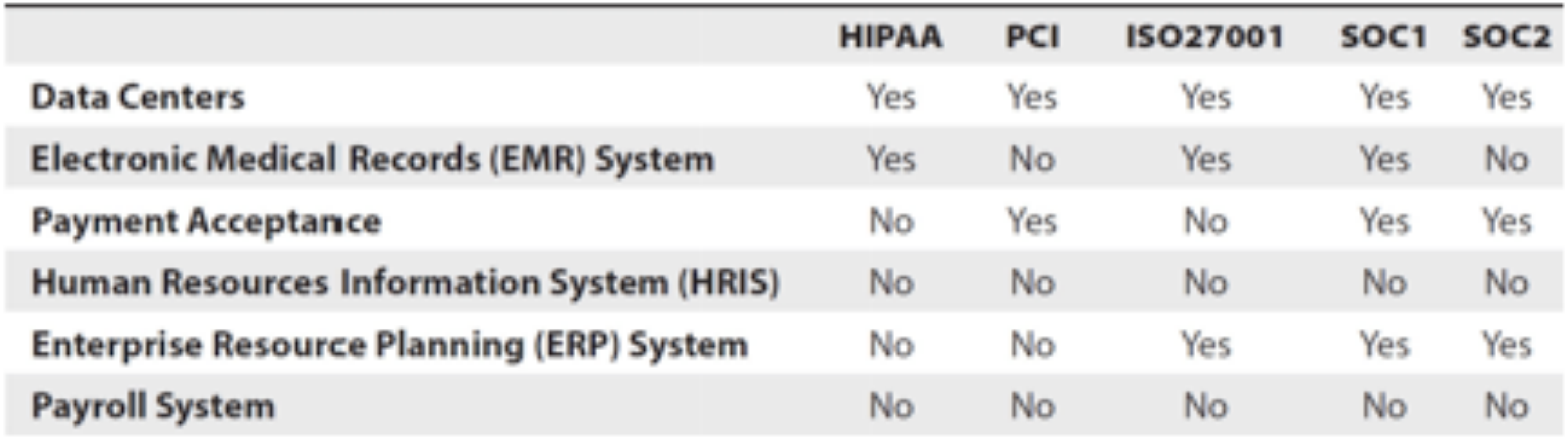
Compliance

- **Conformance to applicable policies, standards, regulations, and other requirements**
- **Security manager must determine whether**
  - **Information systems, processes, and personnel**
  - **conform to those things**

Compliance or Security

- Two categories of organizations
  - Compliance based
    - "Check the box"
    - Do the bare minimum
  - Security and risk based
    - Perform risk assessments, etc.

Applicability



	HIPAA	PCI	ISO27001	SOC1	SOC2
Data Centers	Yes	Yes	Yes	Yes	Yes
Electronic Medical Records (EMR) System	Yes	No	Yes	Yes	No
Payment Acceptance	No	Yes	No	Yes	Yes
Human Resources Information System (HRIS)	No	No	No	No	No
Enterprise Resource Planning (ERP) System	No	No	Yes	Yes	Yes
Payroll System	No	No	No	No	No

Compliance Risk

- Risk from failure to comply
  - With an applicable law or other legal obligation
- Risks may include
  - Sensitive data exposure
  - Fines and sanctions

Compliance Enforcement

- **Audits, control self-assessments, and other examinations of systems and processes**
- **Reveal both direct risks and compliance risk**

Administrative Activities
Personnel Management

Finding and Retaining Talent

- **Shortage of skilled workers**
- **Retaining talent is a challenge**
  - **They get bored and seek new challenges**
- **Look within your organization**
  - **Cross over from IT to information security**

Roles and Responsibilities

- **Role**
  - **A designation that denotes a set of responsibilities**
  - **Examples: *security manager*, *security engineer*, *security analyst***
- **Responsibility**
  - **A stated expectation of activities and performance**
  - **Examples: weekly scans, risk assessments, access requests**

Defining Roles and Responsibilities

- Security manager
  - Analyzes the required activities in the security team
  - Groups them along with
    - Subject matter, skill levels, and other considerations
  - Gives them roles and job titles

Job Descriptions

- Formal description of a position, including
  - Job title
  - Work experience requirements
  - Knowledge requirements
  - Responsibilities

Culture

- **Attitudes, practices, communication styles, ethics, etc.**
- **Many organizations don't regard information security as important**
- **So the security manager must promote security awareness in subtle ways**
- **Developing a "culture within a culture"**

Professional Development

- **Constant learning**
- **This is combat**
- **The adversaries are constantly improving**

Career Paths

- **Most security workers change companies every two years**
  - **To advance to the next level**
- **Providing a career path can prevent that**

Specialties

- Risk management
- Risk analysis
- Information systems auditing
- Penetration testing
- Malware analysis
- Security engineering
- Secure development
- Mobile device security
- Telecommunications and network security
- Social engineering
- Security awareness training
- Forensics
- Cryptography
- Business continuity planning and disaster recovery planning
- Identity and access management
- Threat intelligence
- Third-party risk
- Privacy

Certifications (Non-Vendor)

- Security+
    - Entry-level
- SSCP from (ISC)²
    - More technical than CISSP
- GIAC from SANS
- CEH from EC-Council
- CCSP from Cloud Security Alliance

Certifications (Non-Vendor)

- **CISSP from (ISC)^2**
  - **Essential. Non-technical.**
- **CSSLP (Certified Secure Software Lifecycle Professional) from (ISC)^2**
  - **Essential. Non-technical.**

Certifications (Non-Vendor)

- **ISACA Certifications**
  - **CISM (Certified Information Security Manager)**
  - **CISA (Certified Information Systems Auditor)**
  - **CRISC (Certified in Risk and Information Systems Control)**

Certifications (Vendor)

- **Check Point Certified Security Administrator (CCSA)**
- **Certified Forensic Security Responder (CFSR) from Guidance Software**
- **Radware Certified Security Specialist (RCSS)**
- **Metasploit Certified Specialist from Rapid7**
- **WhiteHat Certified Secure Developer**

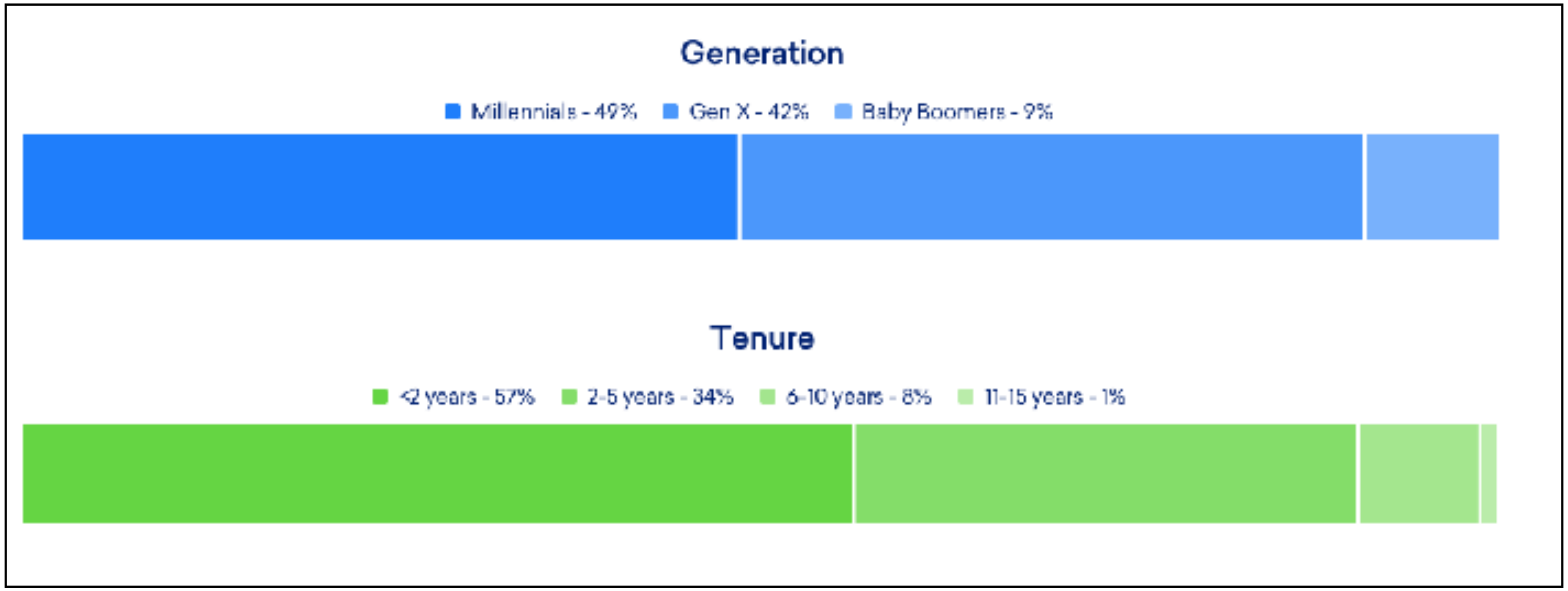
Training

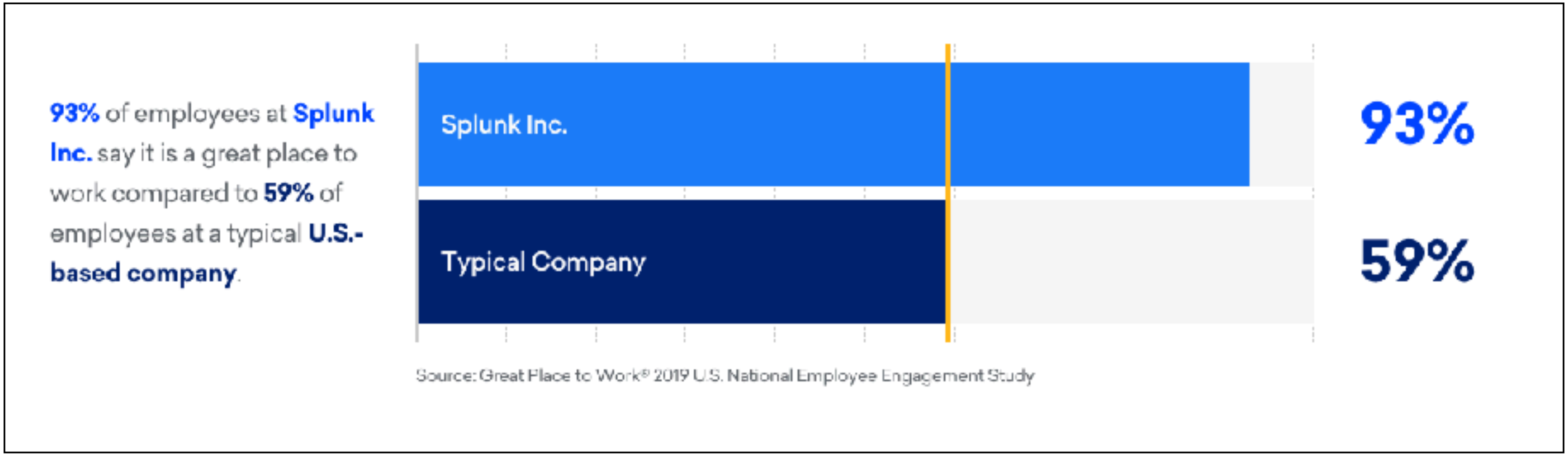
DILBERT
BY SCOTT ADAMS
I NEED TO GET THIS TECHNOLOGY CERTIFICATION.
DilbertCartoonist@gmail.com
WHOA! NO WAY.
IF I PAY FOR YOUR TRAINING, YOU'LL USE YOUR CERTIFICATION TO GET A BETTER JOB.
© 2012 Scott Adams, Inc. /Dist. by Universal Uclick
AT THE MOMENT, YOU'RE IN WHAT WE MANAGERS CALL THE GOLDILOCKS ZONE.
YOU'RE NOT HOT ENOUGH TO GET A BETTER JOB, AND YOU'RE NOT YET INCOMPETENT AT THE ONE YOU HAVE.
WHEN YOUR SKILLS EXPIRE, IN THE NEXT YEAR OR TWO, I'LL REPLACE YOU WITH SOMEONE YOUNGER.
YOU'RE A MONSTER! I'LL PAY FOR MY OWN TRAINING AND LEAVE YOU TO MARINATE IN YOUR OWN STENCH!
www.dilbert.com
6-10-12
HOW DID YOU KEEP YOUR TRAINING EXPENSES SO LOW?
I MARI-NATED IN MY OWN STENCH.

Training

- Minimum: one week
- Often employers reimburse college tuition
- I know DriveSavers gives six weeks of training a year
  - Employees stay there for decades

Splunk




93% of employees at **Splunk Inc.** say it is a great place to work compared to **59%** of employees at a typical **U.S.-based company**.

Source: Great Place to Work® 2019 U.S. National Employee Engagement Study

From https://www.greatplacetowork.com/certified-company/1300565

Kahoot!

Ch 4d-1

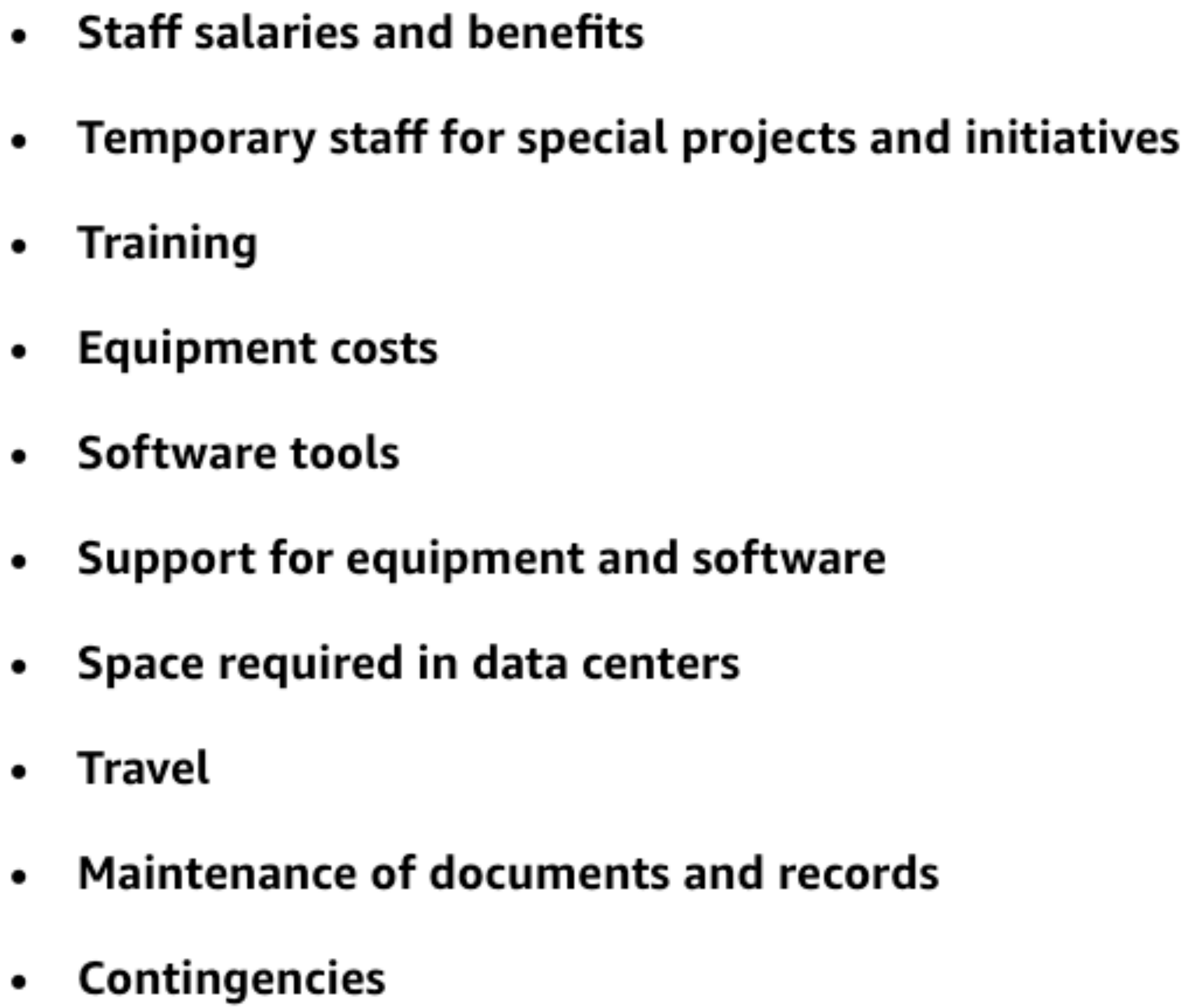
Administrative Activities
Project and Program Management

Projects

- The field is in continuous change
- Project
  - A group activity to achieve a particular aim
- Program Management
  - Management of several concurrent projects

Administrative Activities Budget

Activities to Include



- Staff salaries and benefits
- Temporary staff for special projects and initiatives
- Training
- Equipment costs
- Software tools
- Support for equipment and software
- Space required in data centers
- Travel
- Maintenance of documents and records
- Contingencies

Return on Security Investment (ROSI)

- **Security improvements don't increase revenue or lower costs**
- **The benefit is risk reduction**
- **Difficult to justify to management**

Administrative Activities
Business Case Development

Business Case

- The rationale for making a business investment
- Used to justify making an investment
  - And to support management of the investment later
- Explains the benefits of the investment

Feasibility

- Feasibility study
  - Defines the business problem
  - Describes a number of potential solutions
- Business case should go further
  - And include figures for costs and benefits

Business Case Contents

- **Business problem**
- **Feasibility study results**
- **Increased revenue or efficiency analysis**
- **High-level project plan**
  - **Timeline and number of people**
- **Budget**
- **Metrics**
- **Risks**

Administrative Activities
Vendor Management

Trust Relationships

- Security managers need deep, trusted relationships with security services vendors
- Must confide challenges to a vendor
- And get advice that will benefit the business
  - Not just make a sale

Security Program Operations

Security Program Operations Topics

- **In this lesson**
  - **Event Monitoring**
  - **Vulnerability Management**

Security Program Operations Topics

- **For future lessons**
  - **Secure Engineering and Development**
  - **Network Protection**
  - **Endpoint Protection and Management**
  - **Identity and Access Management**

Security Program Operations Topics (continued)

- **For future lessons**
  - **Security Incident Management Security Awareness Training**
  - **Managed Security Service Providers (MSSPs)**
  - **Data Security**
  - **Business Continuity Planning**

Event Monitoring

Log Reviews

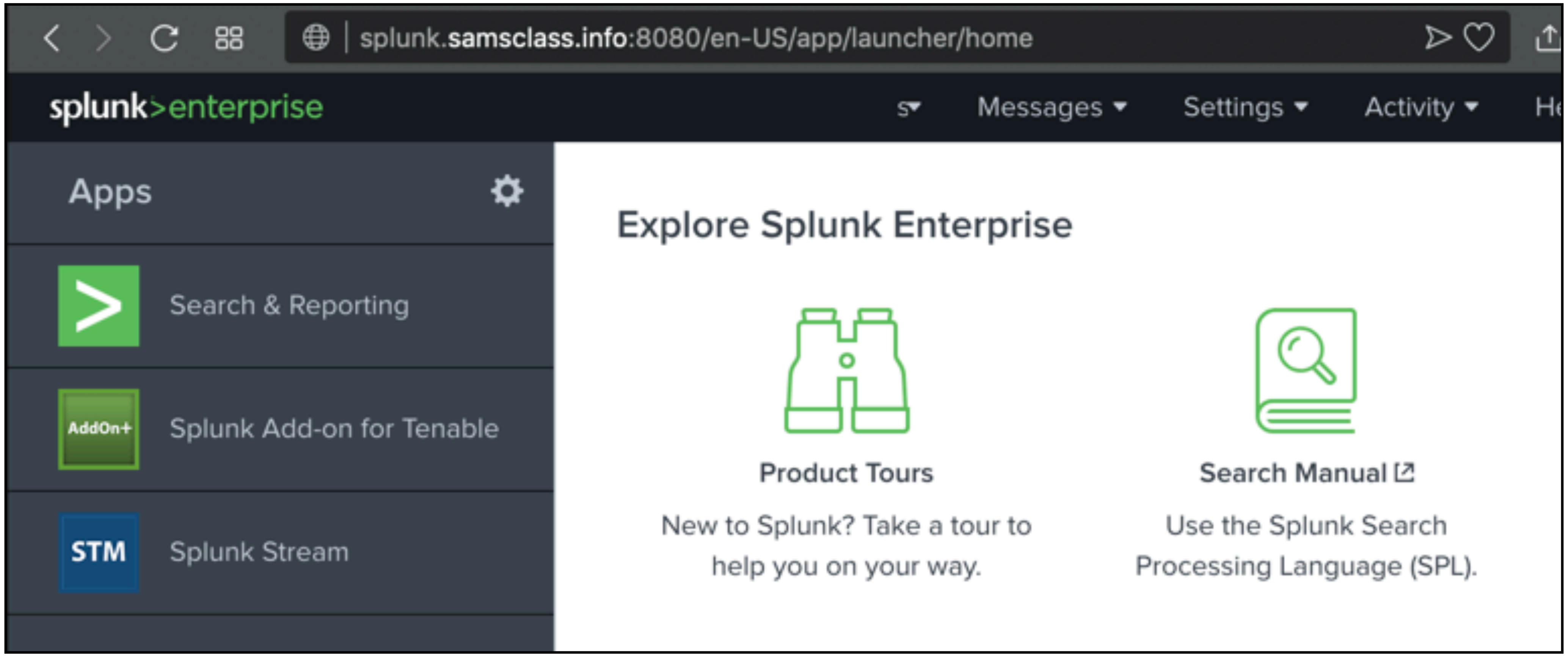
- **Many devices have logs**
  - **Firewalls, servers, operating systems...**
- **Log review used to be a daily activity**
- **Now most organizations perform *real-time event monitoring***

Centralized Log Managment

- **All the events are sent to a *log server***
- **Archives events so they can be reviewed**
- **Used by the SEIM (next slide)**

SEIM (Security Event and Incident Management)

- A system that correlates events from many sources
- Splunk is the industry leader



Explore Splunk Enterprise

New to Splunk? Take a tour to help you on your way.

Use the Splunk Search Processing Language (SPL).

Threat Intelligence

- **SIEMs can ingest threat intelligence feeds**
- **External sources of adversary information**
  - **Such as IP addresses of known attackers**

Orchestration

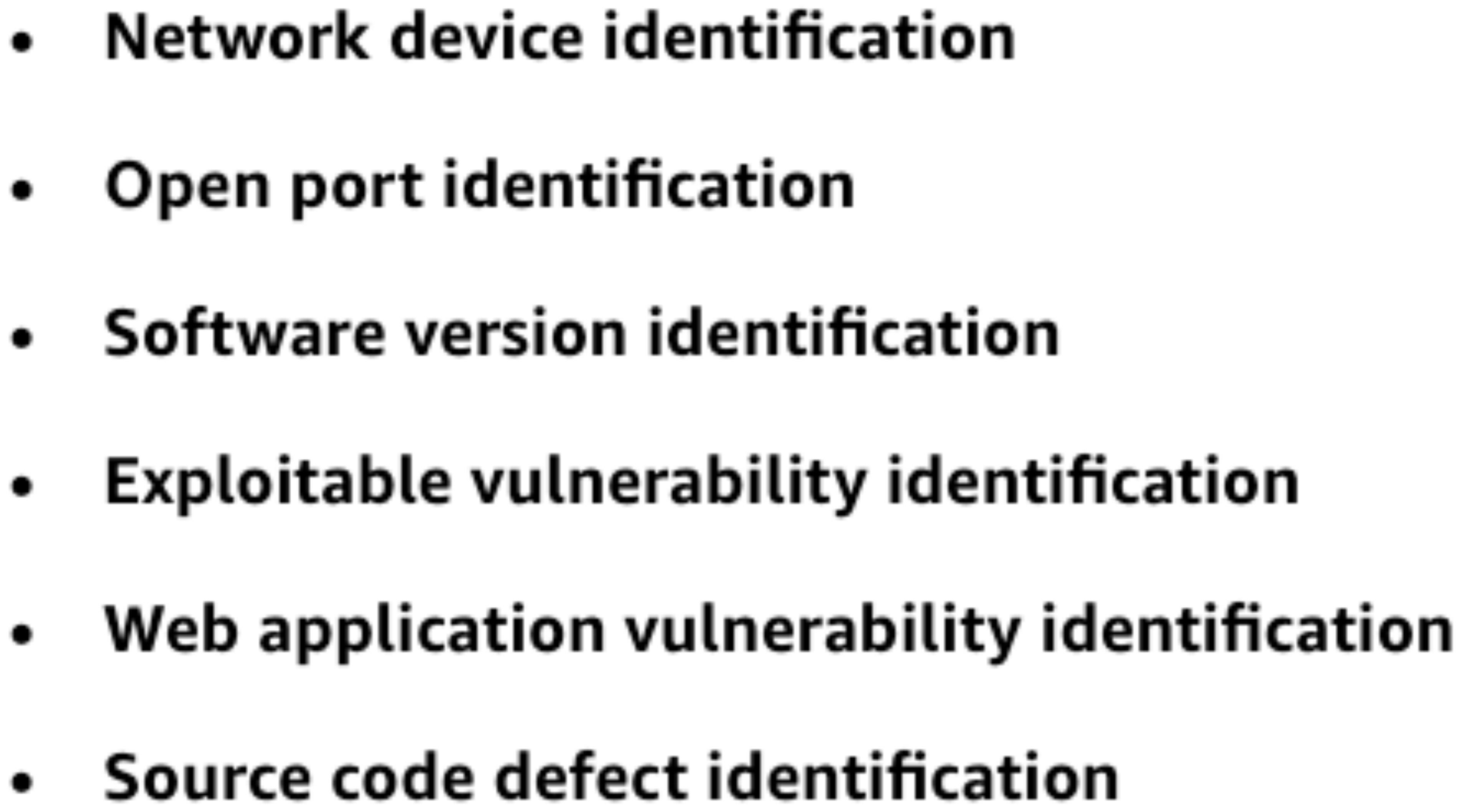
- A scripted, automated response
  - Automatically or manually triggered when specific events occur
- Automates repetitive tasks
- Makes response much faster

Security Program Operations
Vulnerability Management

Vulnerability Managment

- **The practice of periodically examing information systems**
  - **To discover exploitable vulnerabilities**
  - **With analysis and decisions about remediation**

Scanning Tools



- Network device identification
- Open port identification
- Software version identification
- Exploitable vulnerability identification
- Web application vulnerability identification
- Source code defect identification

Vulnerability Management Activities

- **Periodic scanning**
- **Analysis of scan results**
  - **Common Vulnerability Scoring System (CVSS)**
  - **Contextual criticality**
- **Delivery of scan results to asset owners**
- **Remediation**

Common Vulnerability Scoring System (CVSS)

- **Open framework**
- **Rates vulnerabilities from 0 to 10**
- **Includes exploitability, impact, and complexity**

Vulnerability Identification Techniques

- **Security scan**
  - **With an automated tool**
- **Penetration test**
  - **People simulating an attacker**
- **Social engineering assessment**
  - **Phishing or other attacks against humans**

Patch Management

- **Adding vendor patches to IT systems, tools, and applications**
  - **Only the smallest organizations can do it manually**
  - **Automated tools ensure that all systems are patched consistently**

Kahoot!

Ch 4d-2