Applied Virtual Networks

COMP 4912

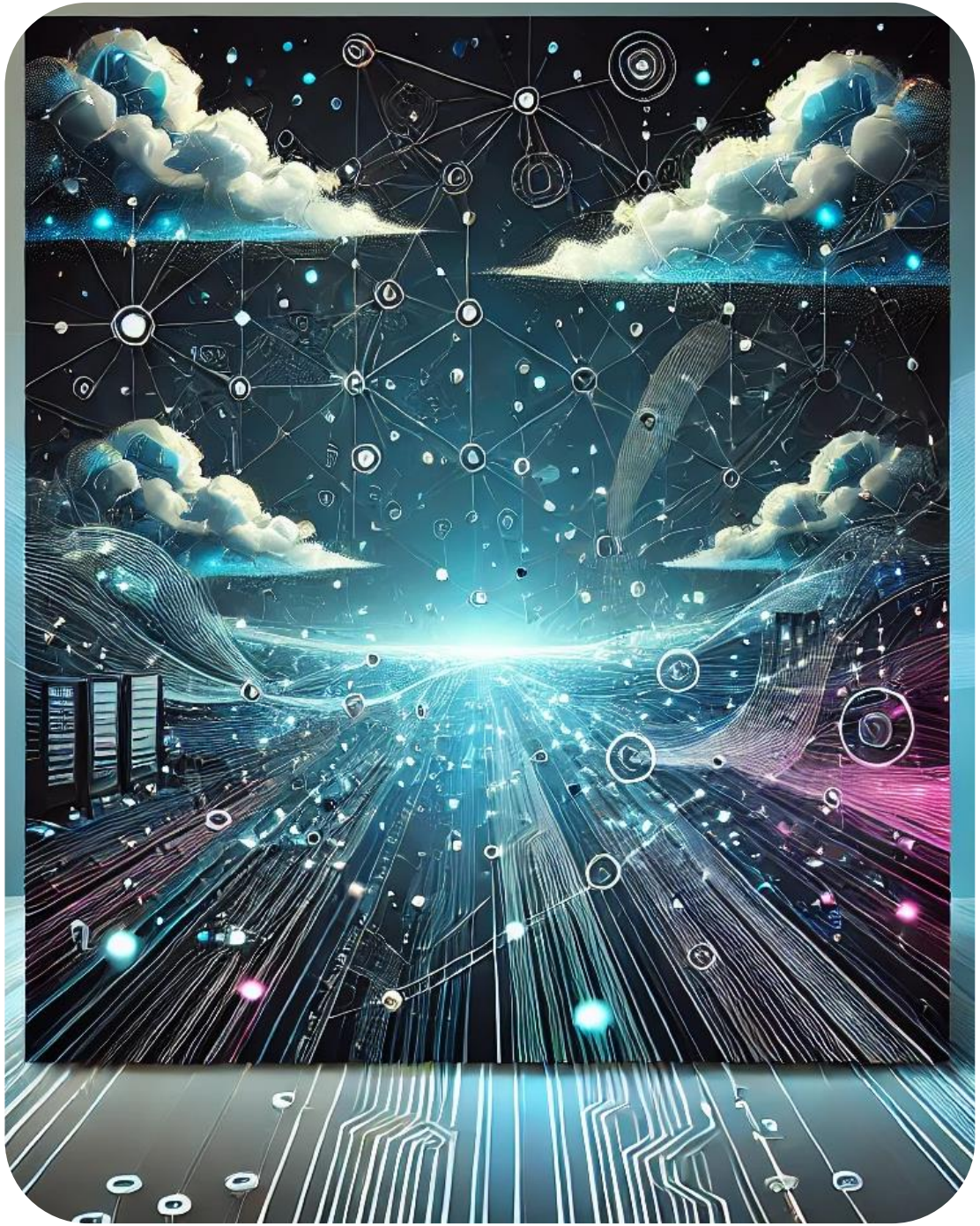
Instructor: **Dawood Sajjadi**

PhD, SMIEEE, CISSP

ssajjaditorshizi@bcit.ca

Winter-Spring 2025

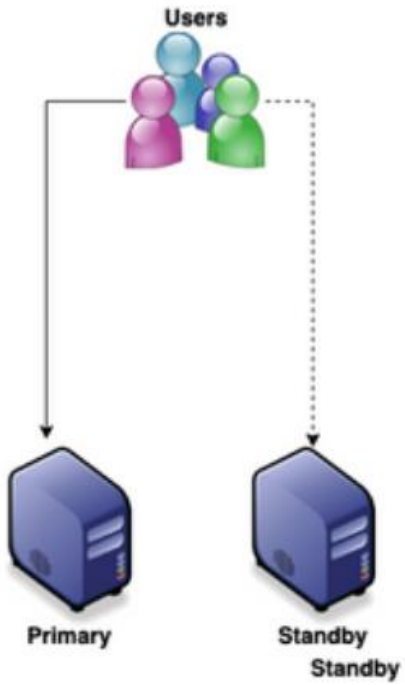
Week #10



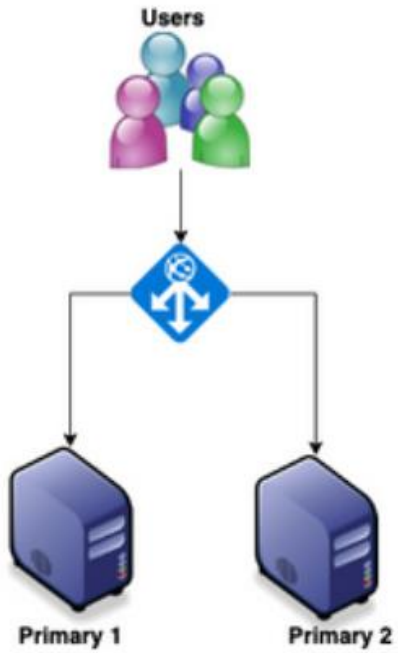
HA vs. FT vs. DR

RECAP

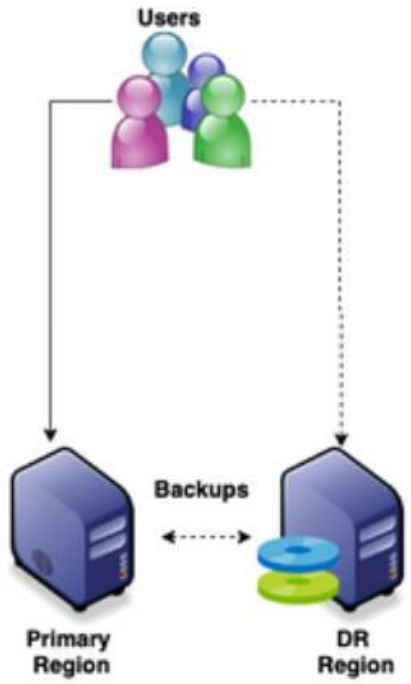
High Availability



Fault Tolererance



Disaster Recovery



BCIT™

Metrics for Service Monitoring

RECAP

There are several known metrics that help to define service **Reliability, Availability, and Disaster Recovery strategies.**

SLO (Service Level Objective)

- ✓ A **targeted performance goal** used internally by service teams.
- ✓ Defines desired service levels (Latency < 100ms, or Uptime > 99.95%).

SLA (Service Level Agreement)

- ✓ A **formal contract** between a service provider and a customer.
- ✓ Defines **minimum service guarantees** (e.g., 99.99% uptime).
- ✓ Includes **penalties** if the provider fails to meet commitments.

RPO (Recovery Point Objective)

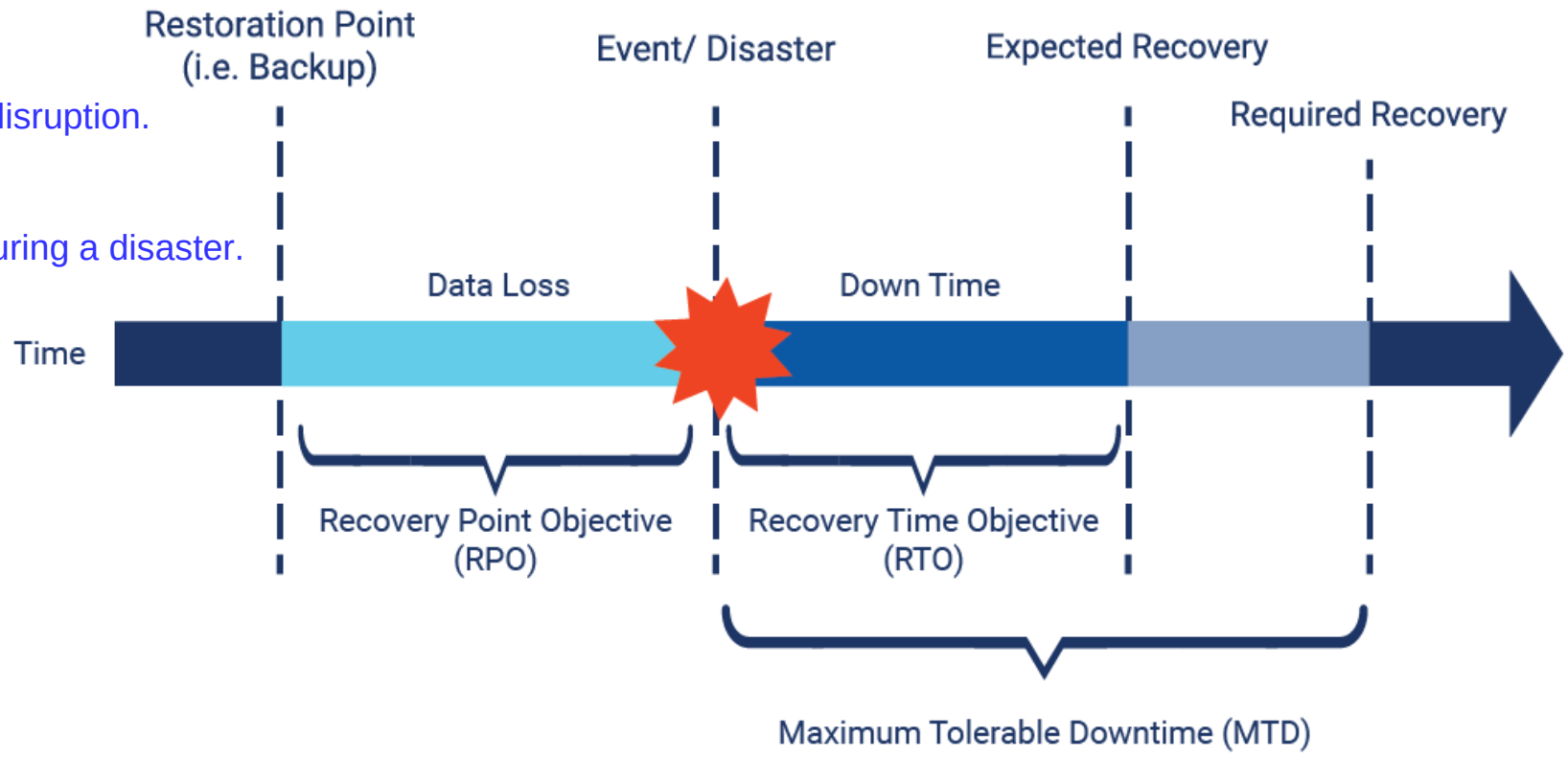
Maximum amount of data loss a company can tolerate.

RTO (Recovery Time Objective)

Maximum time allowed to restore operations after a disruption.

RSL (Recovery Service Level)

The percentage of a service that must be available during a disaster.



BCIT™

Five-Nine SLA (99.999%)

RECAP

$$\text{Availability (\%)} = \left(\frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}\right) \times 100$$

Higher MTBF → Fewer failures → Better uptime
Lower MTTR → Faster recovery → Better uptime

MTBF (Mean Time Between Failures)

- ✓ The **average time a system runs before experiencing a failure**.
- ✓ A higher MTBF means **fewer failures**, increasing overall uptime.
- ✓ Example: If a server has an **MTBF of 200,000 hours**, it fails less frequently.

MTTR (Mean Time To Repair)

- ✓ The **average time taken to repair and restore service after a failure**.
- ✓ A lower MTTR **reduces downtime**, improving availability.
- ✓ Example: If an incident occurs and the service is restored in **5 minutes**, it helps maintain high uptime.

	Availability	Downtime / Year	Downtime / Month	Downtime / Week	Downtime / Day
5 nine	99.999%	5.256 Minutes	0.438 Minutes	0.101 Minutes	0.014 Minutes
	99.995%	26.28 Minutes	2.19 Minutes	0.505 Minutes	0.072 Minutes
4 nine	99.990%	52.56 Minutes	4.38 Minutes	1.011 Minutes	0.144 Minutes
	99.950%	4.38 Hours	21.9 Minutes	5.054 Minutes	0.72 Minutes
3 nine	99.900%	8.76 Hours	43.8 Minutes	10.108 Minutes	1.44 Minutes
	99.500%	43.8 Hours	3.65 Hours	50.538 Minutes	7.2 Minutes
	99.250%	65.7 Hours	5.475 Hours	75.808 Minutes	10.8 Minutes
2 nine	99.000%	87.6 Hours	7.3 Hours	101.077 Minutes	14.4 Minutes

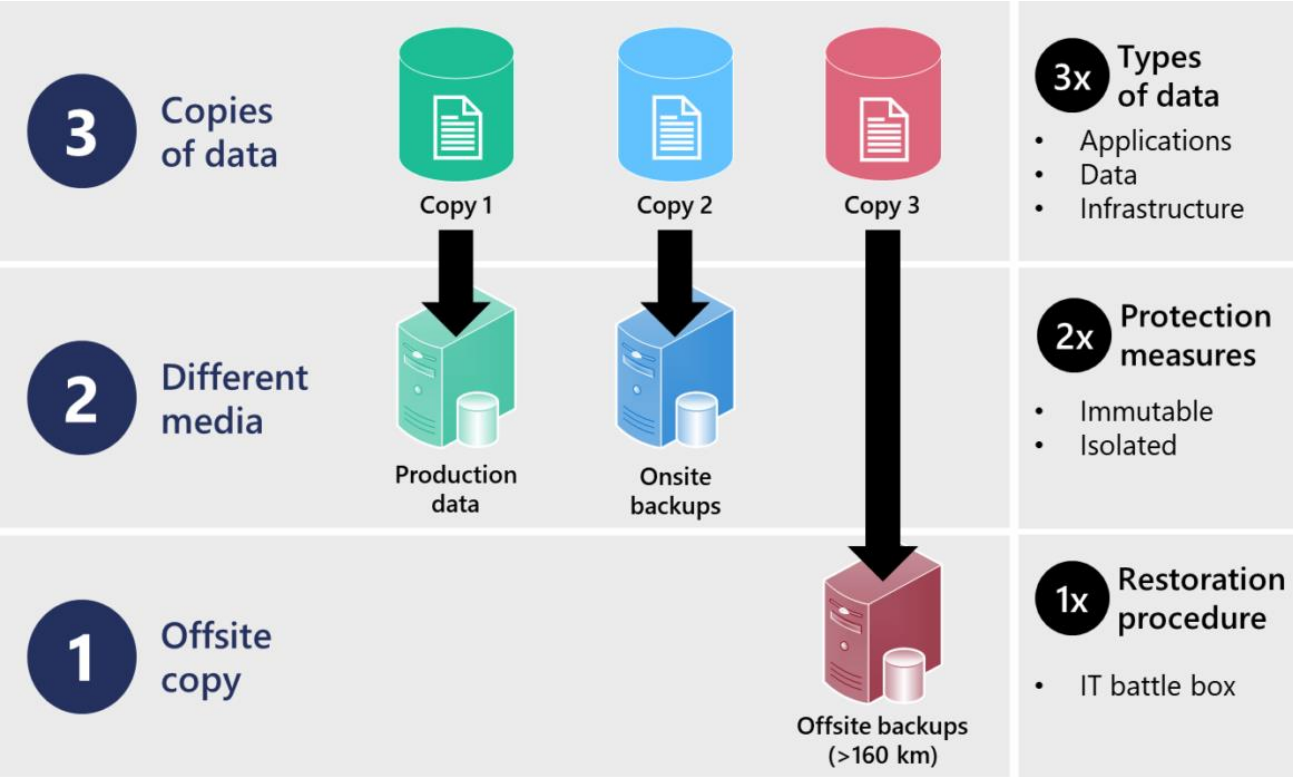
https://aws.amazon.com/blogs/publicsector/achieving-five-nines-cloud-justice-public-safety/

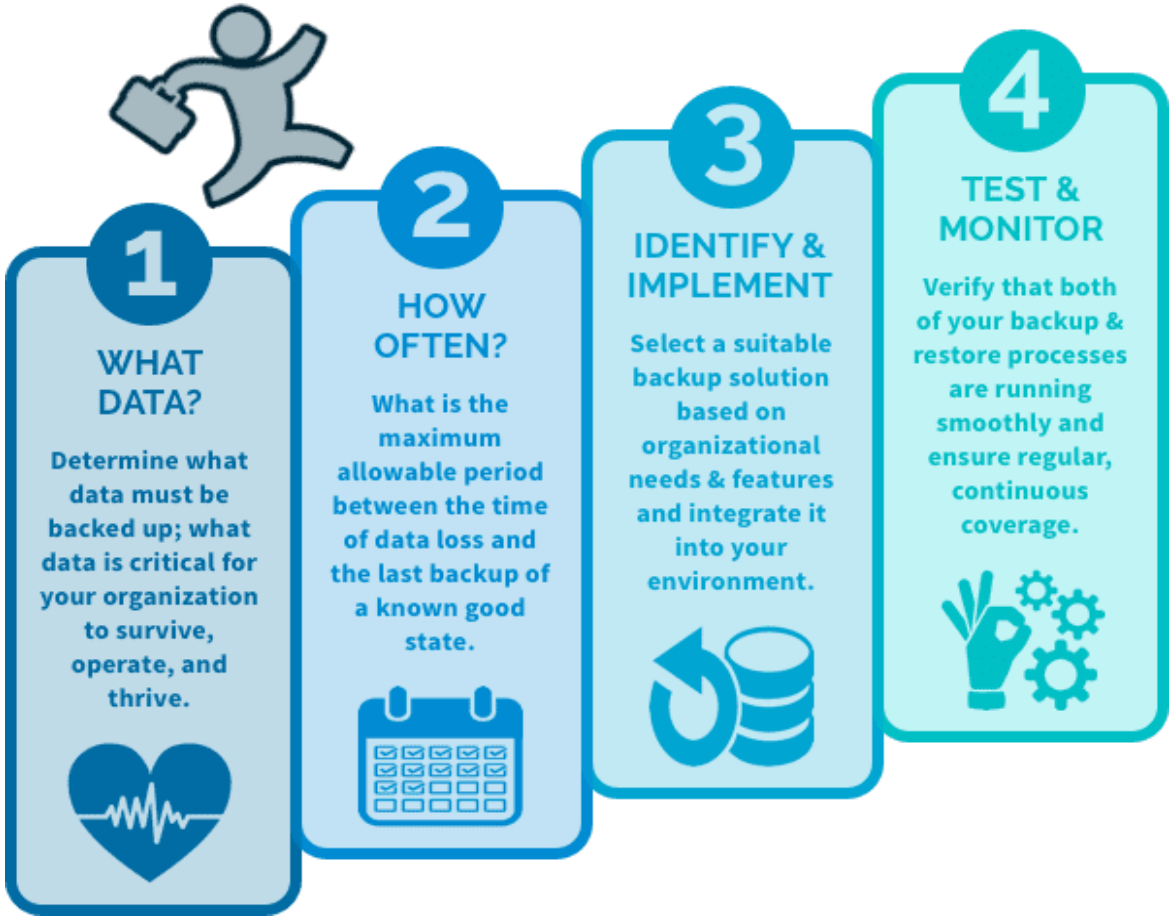
BCIT™

Backup Strategies

RECAP

3-2-1 Backup Rule

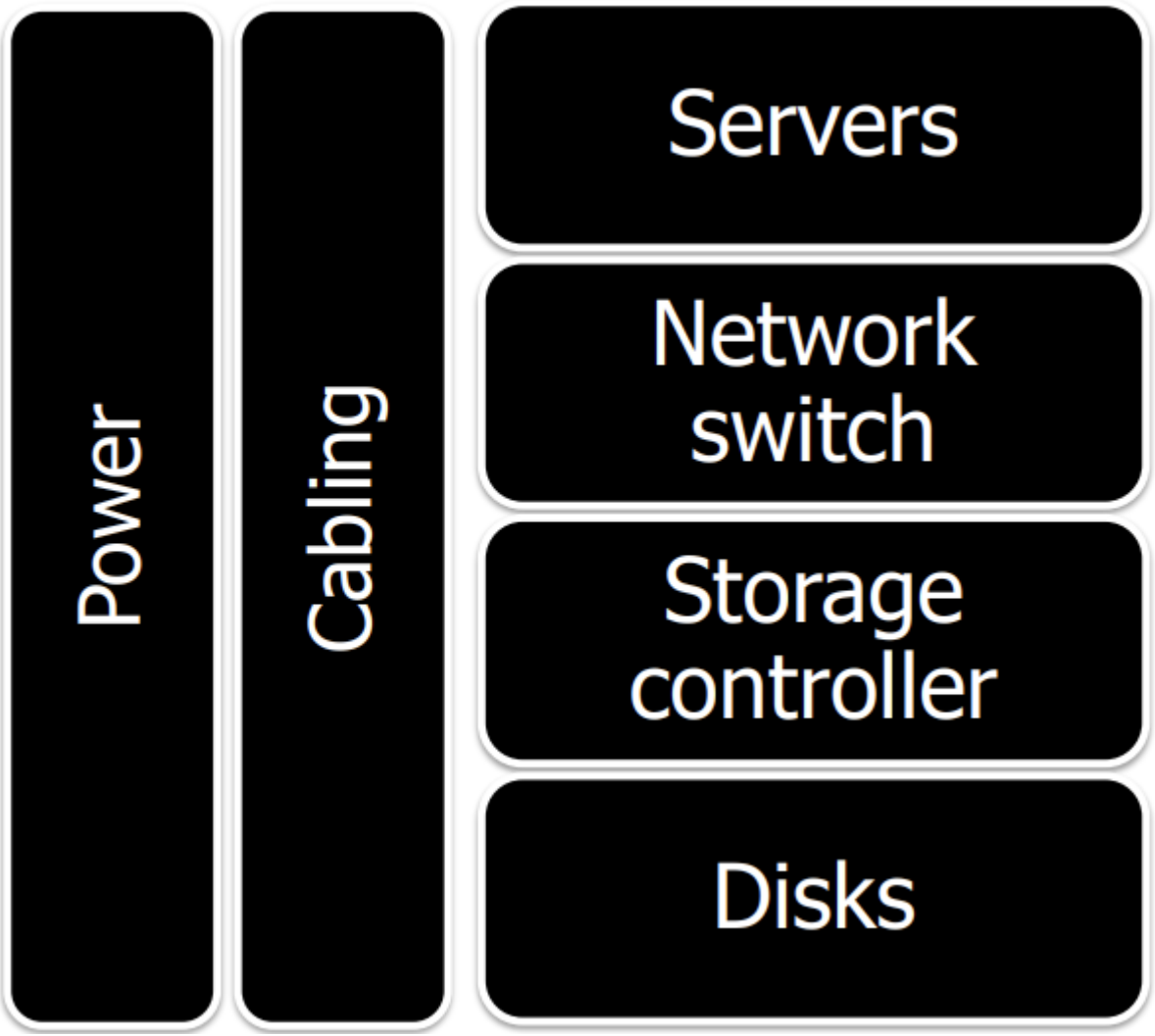


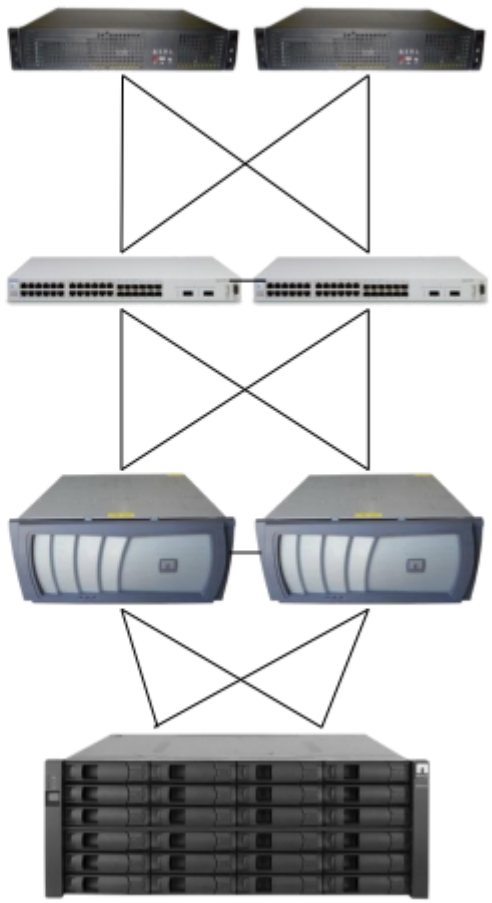


BCIT™

Complete Redundancy

RECAP





https://people.duke.edu/~tkb13/courses/ece566-2020fa/slides/09-ha.pdf

Learning Outcomes of Week #10

1. Understand the core concepts of Cybersecurity.
2. Better understanding about Threat Landscape and Emerging Threats.
3. Explaining key factors to consider for building a Secure Infrastructure.
4. Understanding major elements to build a Secured Virtualized Environment.
5. Describing the roles of Security Compliances and Standards.

BCIT™

Cyber Security

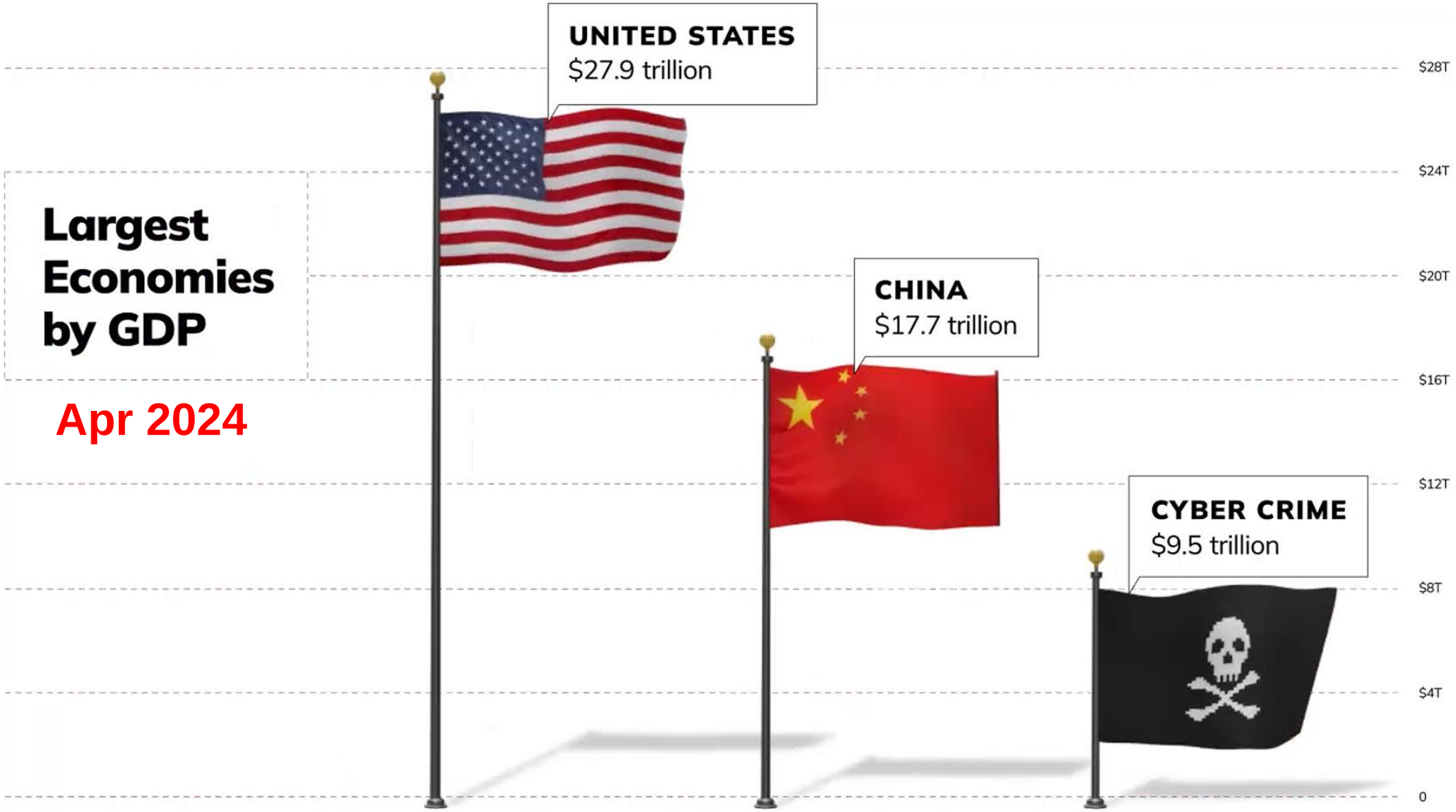
Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.

Key Areas

- ✓ Application Security
- ✓ Information Security
- ✓ Network Security
- ✓ Operational Security

BCIT™

Cyber Crime: The World’s Third-Largest Economy



BCIT™

Cyber Security

Major Common Threats

- ✓ Phishing
- ✓ Malware/Spyware/Adware…
- ✓ Denial-of-Service (DoS) attack
- ✓ Man-in-the-Middle (MitM) attack
- ✓ Crypto-mining/Crypto-Heist

Impacts

- ✓ Data breaches
- ✓ Financial loss
- ✓ Reputational damage

WannaCry Ransomware Attack

Friday, 12 May 2017

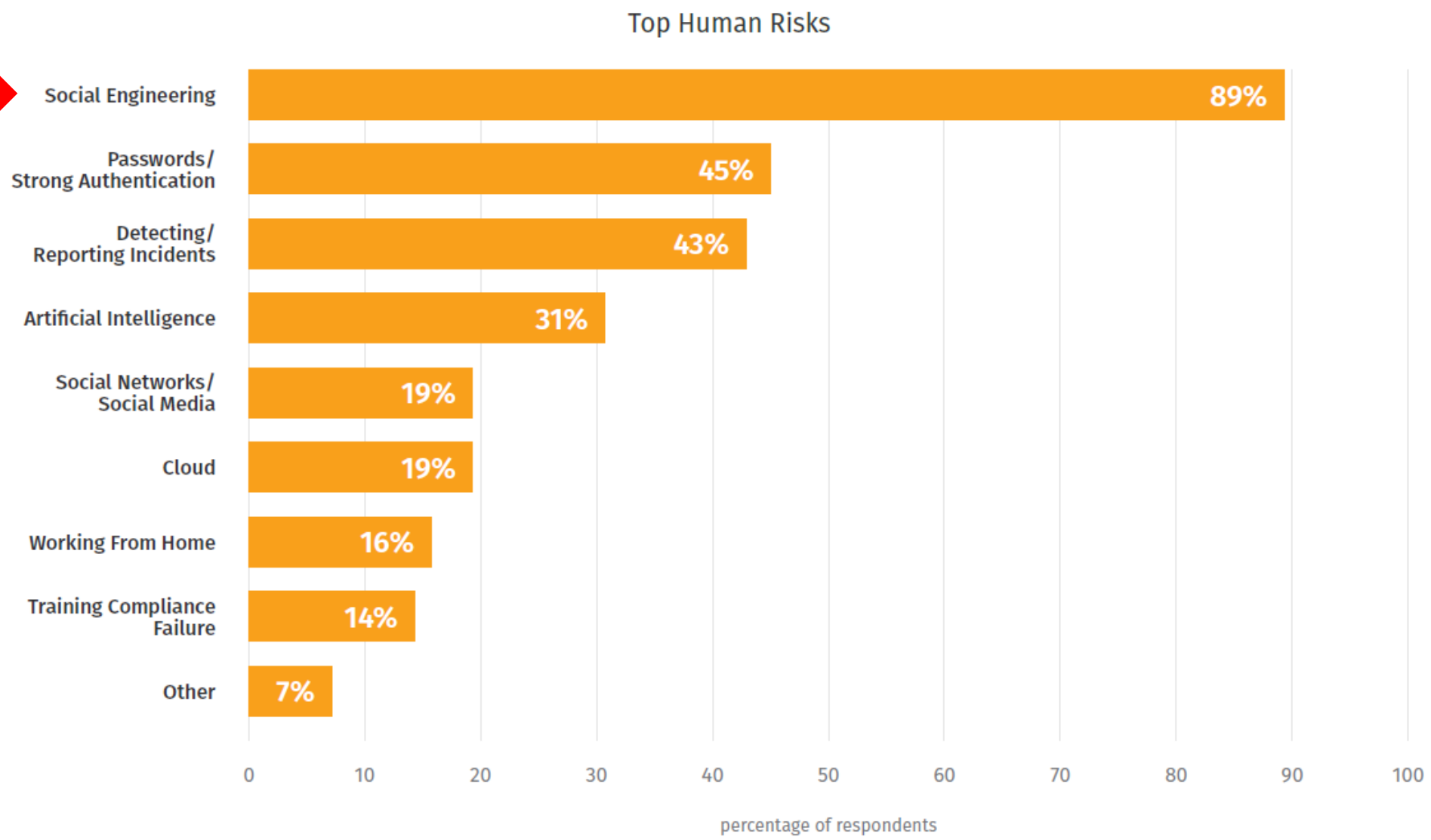
Infected more than **300,000** computers in over **150** countries
[approximate damage: up to $8 billion]

BCIT™

NO ONE is 100% Secure

Top Human Risks – SANS 2024

Social Engineering



Cyber Security

Twitter/X: @5tuxnet

The New York Times

How the Biggest Crypto Heist in History Went Down

The cryptocurrency exchange Bybit lost $1.5 billion to North Korean hackers last month — and it all traced back to an account on a free...

2 weeks ago

Reuters

Crypto's biggest hacks and heists after $1.5 billion theft from Bybit

LONDON, Feb 24 (Reuters) - Cryptocurrency exchange Bybit said last week hackers had stolen digital tokens worth around $1.5 billion,...

3 weeks ago

fbi.gov

March 7, 2025

FBI Denver Warns of Online File Converter Scam

The FBI Denver Field Office is warning that agents are increasingly seeing a scam involving free online document converter tools, and we want to encourage victims to report instances of this scam.

THAILAND SEIZES 3,200 CALLS/SEC SIMBOXES IN CALL CENTER GANG CRACKDOWN

2024

Cyber Security

Twitter/X: @5tuxnet

ZDNet, July 19, 2019

Hackers target 62 US colleges by exploiting ERP vulnerability

Attacks failed; however, the Department of Education is alerting colleges about ongoing ex

Arstechnica, August 2, 2019

New advanced malware, possibly nation sponsored, is targeting US utilities

Law and Crime News

‘Serial hacker’ who created fake death certificate to skirt $116K in child support is headed to prison

Jesse Kipf pleaded guilty in April to hacking into a state database to create a fake death certificate so he would be officially listed as a...

Aug 21, 2024

Reuters, August 8, 2019

Apple offers record 'bounty' to researchers who find iPhone security flaws

up to $ 1 million

The Guardian

London hospitals cancel nearly 1,600 operations and appointments in one week due to hack

London hospitals cancel nearly 1,600 operations and appointments in one week due to hack ... Hospitals in London had to cancel almost 1,600...

Jun 14, 2024

CBC

A huge hack of U.S. phone companies means your text messages may not be safe

Canadians should consider encrypted messaging services to protect themselves, cybersecurity experts say. James Dunne · CBC News · Posted:...

Dec 7, 2024

BBC

What to know about string of US hacks blamed on China

Presidential campaigns and the US telecommunications network have also been targeted by hackers in recent months.

Dec 31, 2024

Los Angeles Times

Hackers may have stolen the Social Security numbers of every American. Here's how to protect yourself

The hacking group USDoD claimed in April to have stolen personal records of 2.9 billion people from National Public Data.

Aug 19, 2024

Cyber Security

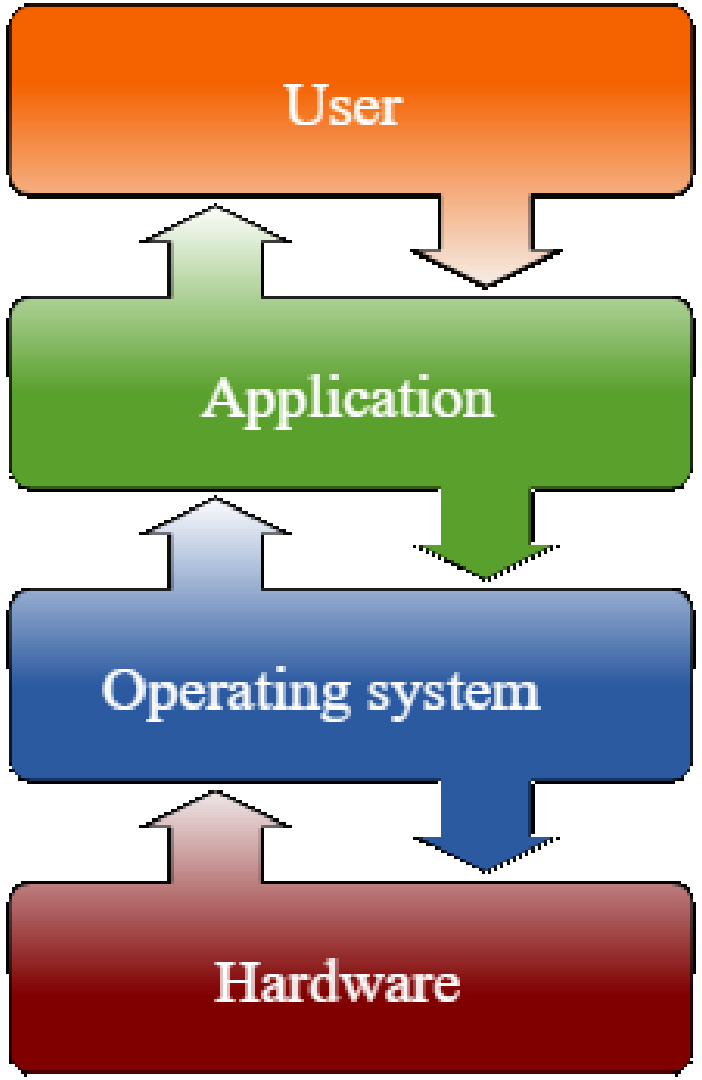
Public Internet

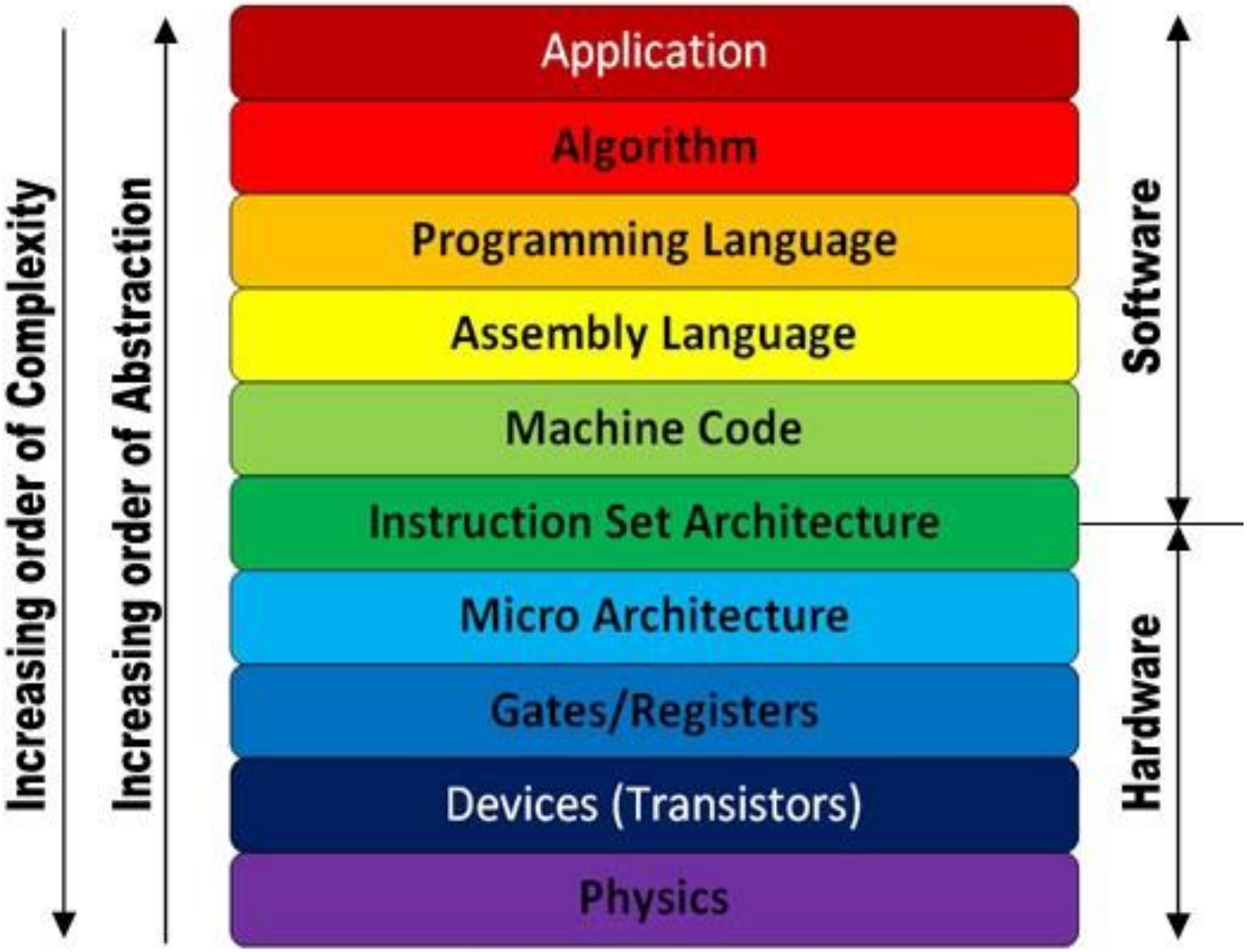
Private Internet

BCIT™

TorProject.org

Cyber Security





BCIT™

Cyber Security

Basic Measures

- ✓ Use strong and unique passwords (password manager)
- ✓ Enable two-factor authentication (2FA)
- ✓ Regularly update your OS/Applications
- ✓ Do Not Install Unknown software

Advanced Measures

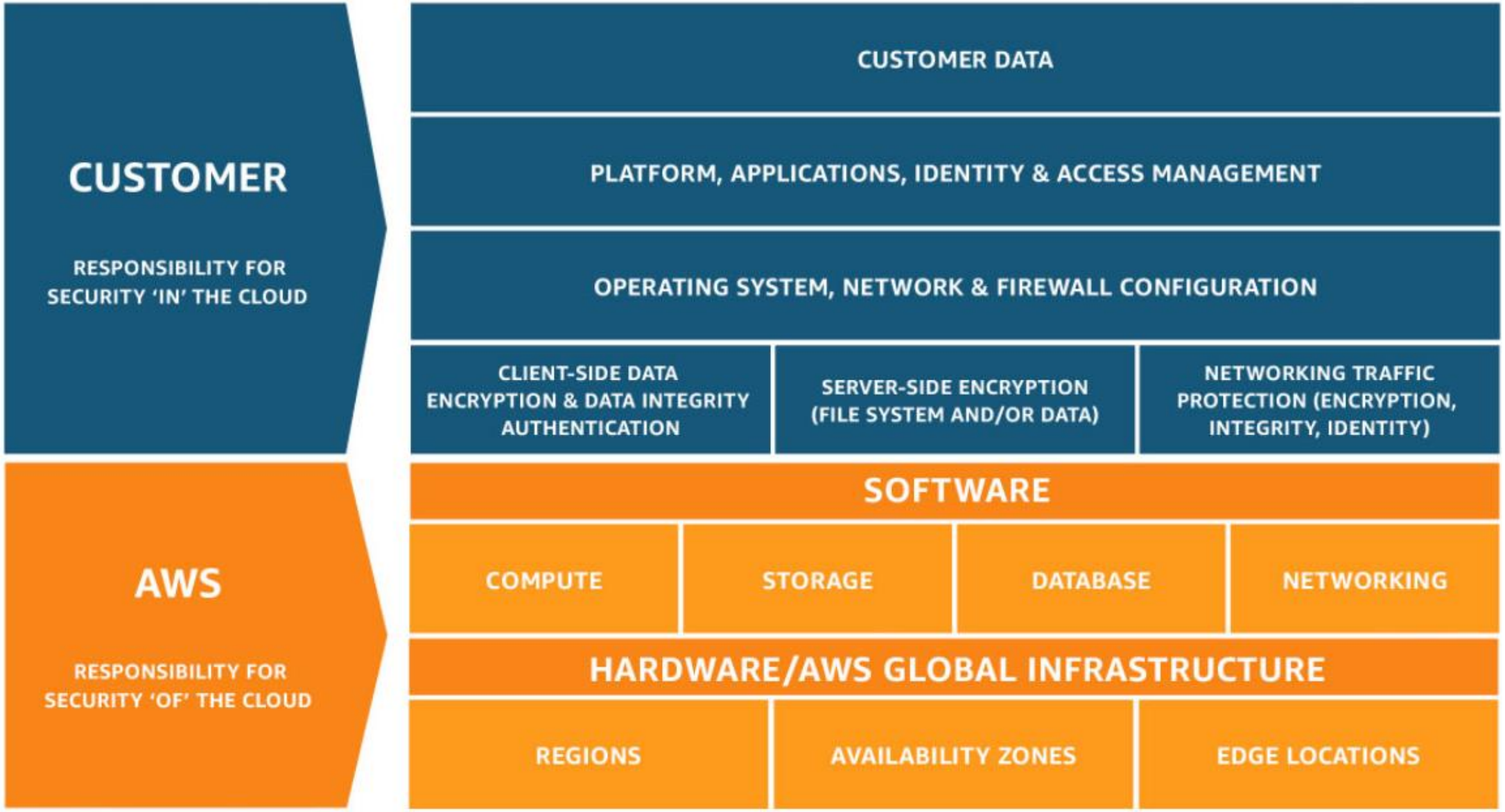
- ✓ Network segmentation
- ✓ Encryption (at-rest, in-transit, in-use)
- ✓ Continuous Monitoring and Incident Response

Role of Individuals

- ✓ Importance of personal responsibility and awareness

BCIT™

Shared Responsibility Model



BCIT™

Shared Responsibility Model

Cloud Security encompasses the technologies, controls, processes, and policies which combine to protect your cloud-based systems, data, and infrastructure.

Cloud Security is a shared responsibility between you and your cloud service provider. You implement a cloud security strategy to protect your data, adhere to regulatory compliance, and protect your customers' privacy.

	Infrastructure-as-a-service (IaaS)	Platform-as-a-service (PaaS)	Software-as-a-service (SaaS)
People	You	You	You
Data	You	You	You
Applications	You	You	CSP
Operating system	You	CSP	CSP
Virtual networks	You	CSP	CSP
Hypervisors	CSP	CSP	CSP
Servers and storage	CSP	CSP	CSP
Physical networks	CSP	CSP	CSP

BCIT™

https://kinsta.com/blog/cloud-security/

Securing your Workloads

https://kinsta.com/blog/cloud-security/

How to Minimize the Risk in Virtualized Environment?

No VM Sprawl: Many VMs created but not managed properly.

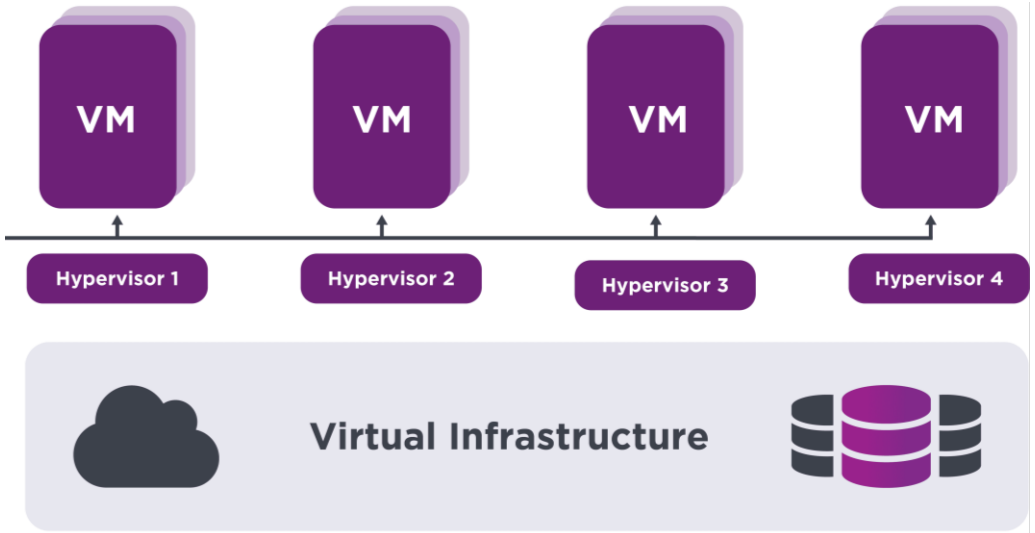
Manage Snapshots: Inappropriate VM Snapshot retention period, may cause Storage overload.

Regular Update of Hypervisor/VMs: To minimize the risk of Security Threats.

Network Segmentation: Isolating critical workload and data from major threats.

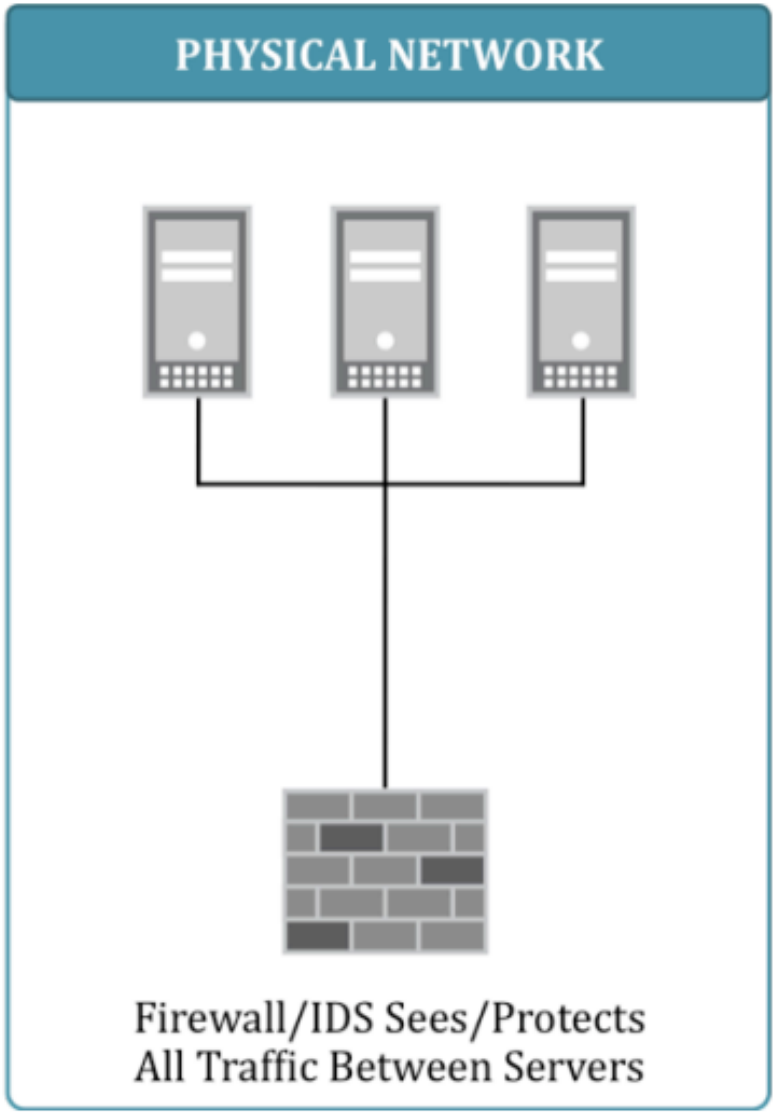
Audit trails and logging: getting a record of specific activities and data within systems.

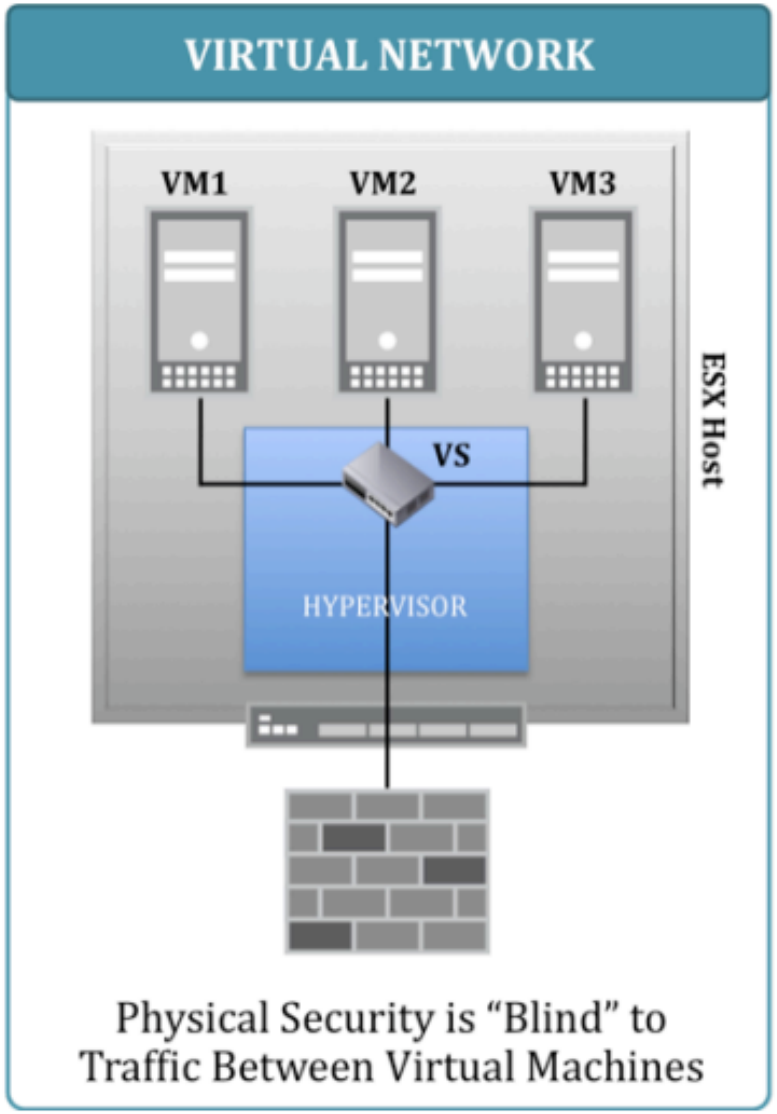
VM Encryption: Protecting sensitive data in case of unauthorized access to VMDK files.



https://www.freecodecamp.org/news/vm-data-protection-best-practices/

VM Security





BCIT™

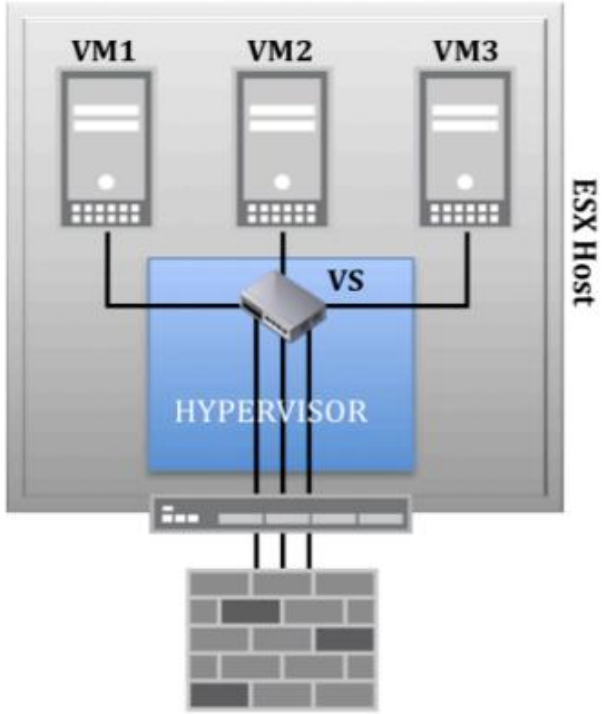
VM Security

1. VLAN Segmentation

Each VM in separate VLAN

Inter-VM communications must route through the firewall

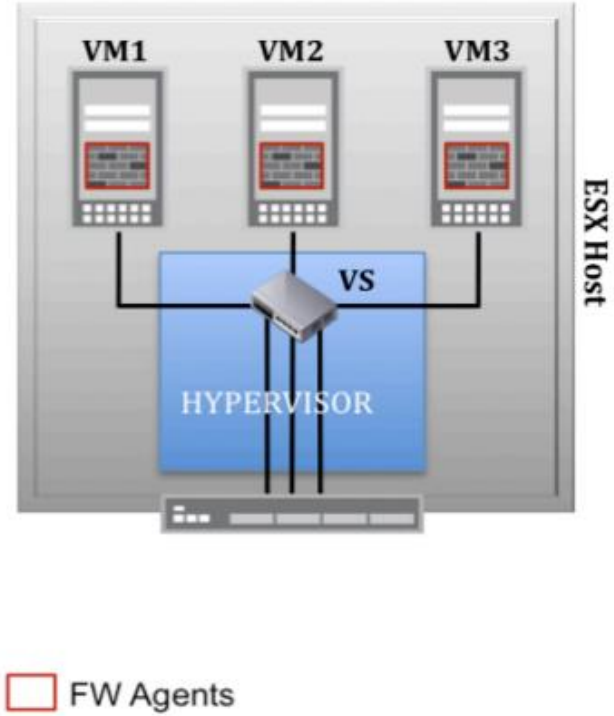
Drawback: Complex VLAN networking; Slow



2. Agent-based

Each VM has a software firewall

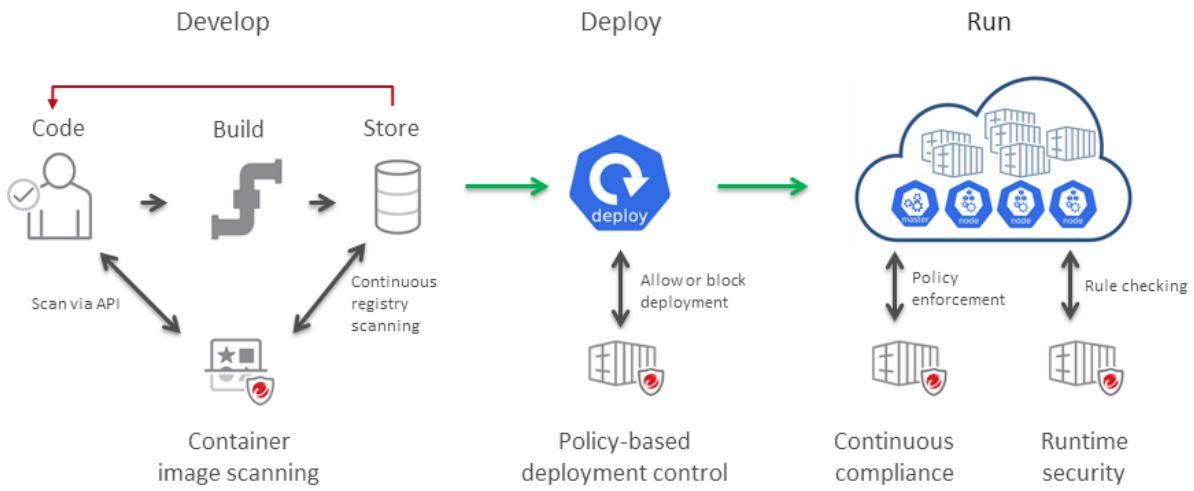
Drawback: Significant performance implications; Huge management overhead of maintaining software and signature on 1000s of VMs



http://viewer.media.bitpipe.com/1215444125_915/1265208156_314/5-Best-Practices-To-Protect-Virtual-Environments.pdf

Container Security

1. Source base image from trusted repositories
2. Install verified packages
3. Minimize attack surface in the image
4. Do not put secrets in the image
5. Use of secure private or public registries
6. Do not use privileged user to run the app in a container
7. Implement image vulnerability scanning in CI/CD
8. Enable kernel security profiles like AppArmor
9. Secure centralized and remote logging
10. Deploy runtime security monitoring



1 — Source Image from Trusted Publishers

Use hardened base images from well-known publishers with the latest security fixes and patches.

2 — Install Verified Packages

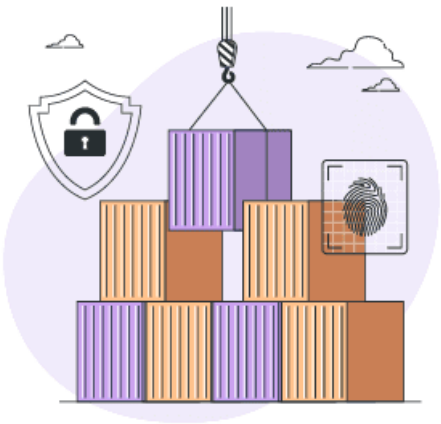
The packages installed on the base image should be from verified and trusted sources.

3 — Minimize Attack Surface

Install the minimum number of packages and libraries in the image to reduce the vulnerability risk.

4 — Do not put Secrets in Image

Keep secrets including passwords, tokens, API keys, etc in the external secret manager for better security.



5 — Use Secure private/ public Registries

Ensure the image is hosted on a secure and trusted registry to prevent unauthorized access.

6 — Disallow Root User to Run the Container

Create an unprivileged user and use it to run the application process inside the container.

7 — Implement Image Vulnerability Scanning

Regularly scan images to identify security vulnerabilities (CVEs) and loopholes.

8 — Enable Kernel Security Profiles

Revoke unnecessary permissions & restrict application access to limited resources.

9 — Secure Centralized & Remote Logging

Securely stream the logs to a centralized system for audit and future forensics.

10 — Deploy Runtime Security Monitoring

Continuously monitor and log the application behavior to prevent and detect malicious activities.

BCIT

https://www.infracloud.io/blogs/top-10-things-for-container-security/

How to Secure a Server?

1. Download the Latest Operating System (OS)
2. Pick your OS/Virtualization Framework, wisely (if not using Bare-metal)
3. Harden your Operating System and Applications (via CIS Controls)
4. Apply IAM/RBAC to Access Server
5. Enable MFA to Access your Server/Service
6. Enable Logging/Auditing (via PAM/Syslog)
7. Setup Network Segmentation and Limit inbound/outbound Traffic via Firewall Policies
8. Implement IDPS and SIEM Solutions in your Network
9. Install EDR/rsyslog/SNMPv3 agent on the Server (for monitoring)
10. Patch your Operating System and Applications on Monthly basis (Patch Tuesday)
11. Regular Security Scanning to find Missed Vulnerabilities and Fix them
12. Schedule regular Backup from your Data on the Server
13. Monitor Server Functionality/Performance/Security
14. Define and Implement Clear Change Control process
15. Encrypt your Data (at-rest/in-transit)
16. Develop a Comprehensive Incident Response Plan for your Server
17. Develop a Comprehensive Disaster Recovery Plan for your Server
18. Use Secure IaC and Version Control to maintain your Server Configuration (GitLab/Jenkins)
19. Avoid Installing Unknown Packages/Libraries on your Server (Supply Chain Controls)
20. Provide a Secure Remote Access Mechanism (VPN/MFA)
21. Deploy Data Loss Prevention (DLP) Solutions to Protect your Data
22. Apply the Best Security Practices/Standards to your environment (ISO27K/SOC2/GDPR)

BCIT™

Enforcing Security Policies

Company
Policies

→ Prepared/Approved by C-level managers

Security
Standards

→ CIS, PCI DSS, HIPAA, GDPR

Procedures
Tools, Controls, Guidelines

→ Detection and Mitigation of Security Risks, Threats and Vulnerabilities

BCIT™

Enforcing Security Policies

CIS® Center for Internet Security®

www.cisecurity.org

Developing the best practice solutions and global security standards as **Security Controls and Benchmarks**

Security **Standards** ⟹ CIS, PCI DSS, HIPAA, GDPR

PCI Security Standards Council®

www.pcisecuritystandards.org

GDPR

General **D**ata **P**rotection **R**egulation

www.gdpr.eu

BCIT™

Regulatory Requirements

1. HIPAA (Health Insurance Portability and Accountability Act)
Ensures the protection of sensitive health information by regulating privacy, security, and data breach notifications. It applies to healthcare providers, insurers, and their business associates.

2. PCI-DSS (Payment Card Industry Data Security Standard)
A security standard designed to protect credit card transactions and prevent fraud. It mandates secure handling, storage, and transmission of cardholder data for businesses that process payments.

3. SOC2 (System and Organization Controls)
A framework for assessing an organization's controls around security, availability, processing integrity, confidentiality, and privacy. It is commonly used for SaaS and cloud service providers.

4. FedRAMP (Federal Risk and Authorization Management Program)
A U.S. government program that standardizes security assessments for cloud service providers. It ensures federal agencies use secure and compliant cloud solutions

5. GDPR (General Data Protection Regulation):
It is a comprehensive data protection law that establishes strict rules for the processing, storage, and transfer of personal data of individuals within the European Union. It mandates that organizations obtain explicit consent for data processing, implement strong data protection measures, and provide individuals with clear rights over their personal information.

6. ISO27000K:
It refers to a family of international standards, including ISO/IEC 27001, that guide organizations in establishing and maintaining robust information security management systems (ISMS). These standards emphasize the importance of risk assessment, continuous improvement, and comprehensive security controls to protect critical information assets.

GRC (Governance, Risk, Compliance)

What is GRC (Governance, Risk, and Compliance)?

GRC (Governance, Risk, and Compliance) is a structured approach that organizations use to align their IT and business strategies with regulatory requirements while effectively managing risks. It consists of three key components, which are as follows:

Governance (G) – Ensures that the organization's operations align with business objectives, ethical standards, and stakeholder expectations.

Risk Management (R) – Identifies, assesses, and mitigates risks that could impact the organization's security, financial health, and reputation.

Compliance (C) – Ensures the organization follows relevant laws, regulations, and industry standards, such as **GDPR**, **ISO-27001**, or **SOC2**.

BCIT™

GRC (Governance, Risk, Compliance)

Why Do Organizations Need GRC?

Regulatory Compliance – Avoids legal penalties and ensures adherence to industry regulations.

Risk Mitigation – Protects against cybersecurity threats, financial losses, and operational risks.

Operational Efficiency – Streamlines internal processes, reducing redundancies and inefficiencies.

Reputation Management – Prevents reputational damage by ensuring ethical and legal business conduct.

Strategic Decision-Making – Provides data-driven insights to align business goals with risk tolerance.

BCIT™

Real World Examples

1 Breakout Rooms

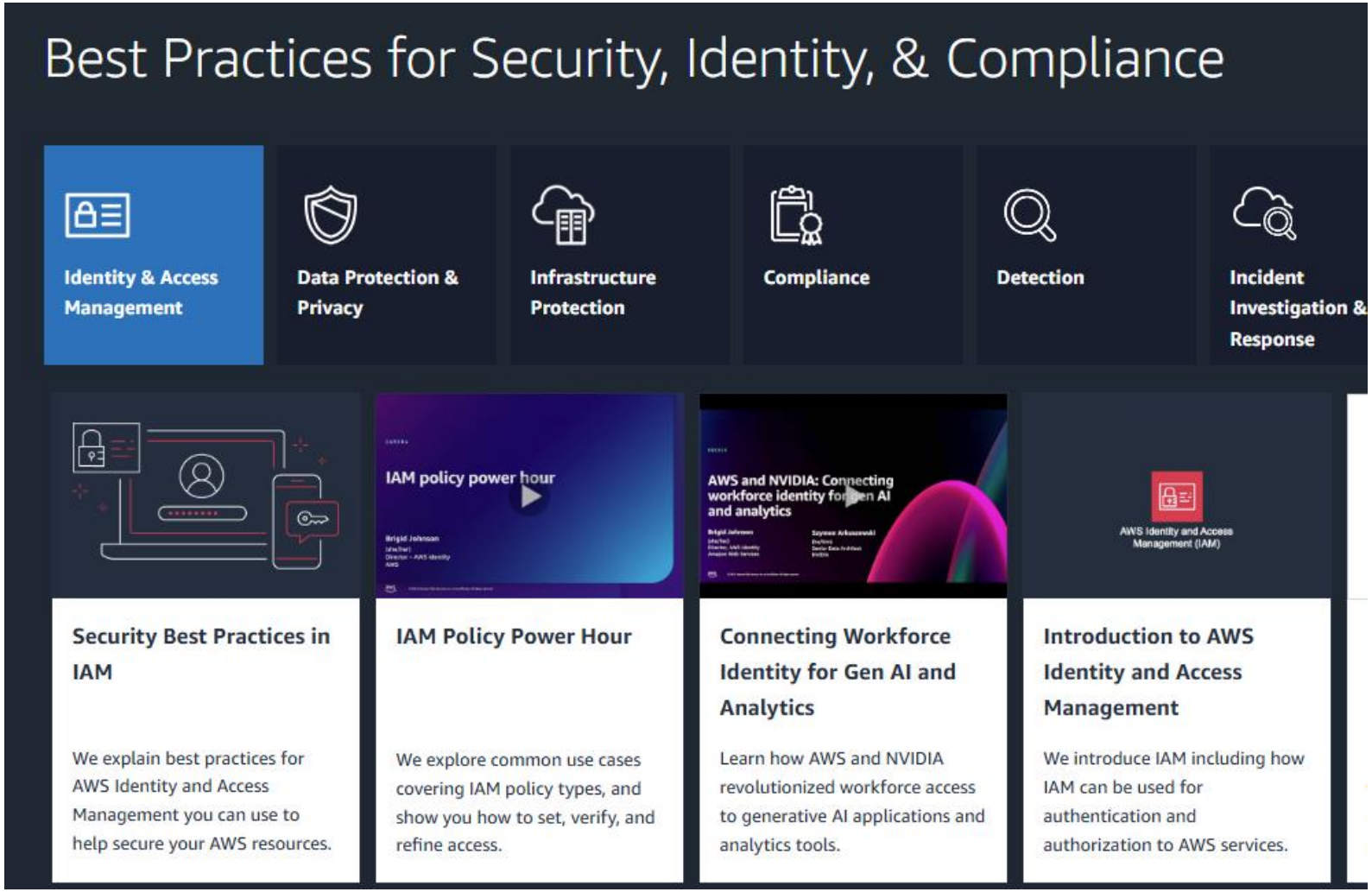
Search for a company or organization that has publicly shared information about a compliance.

SOC2: A cloud service provider might have a dedicated webpage for its SOC2 Type II report, detailing security controls and audit results.
PCI-DSS: A retail company may share how it secures payment transactions and complies with PCI standards to build customer trust.
GDPR: A multinational tech company might describe its data handling policies and user consent processes as part of GDPR compliance.
ISO27K: A financial institution might explain its implementation of an Information Security Management System (ISMS) and its certification journey.

Each student will search for these four points and then they comment on similarities or differences among the standards and how each example underscores the importance of GRC in the modern business environment.

Best Cloud Security Practices

Check https://aws.amazon.com/architecture/security-identity-compliance/



BCIT™

Best Cloud Security Practices

Check https://cloud.google.com/security/best-practices

Google Cloud security best practices center

Explore these best practices for meeting your security and compliance objectives as you deploy workloads on Google Cloud.

Contact us

Best practices guides

Best practices guides provide specific, informed guidance on helping secure Google Cloud deployments and describe recommended configurations, architectures, suggested settings, and other operational advice.

BCIT™

Popular Courses on Cloud/Cyber Security

- 2.1 CertNexus
- 2.2 Cisco Systems
- 2.3 Computing Technology Industry Association (CompTIA)
- 2.4 Council for Registered Ethical Security Testers (CREST)
- 2.5 Certified Wireless Network Professionals
- 2.6 EC Council
- 2.7 Global Information Assurance Certification (GIAC)
- 2.8 Information Systems Audit and Control Association (ISACA)
- 2.9 International Information System Security Certification Consortium (ISC2)
- 2.10 itSM Solutions
- 2.11 McAffee Institute
- 2.12 Offensive Security
- 2.13 PECB
- 2.14 SECO Institute

https://www.cyber.gc.ca/en/guidance/certifications-field-cyber-security

Real World Examples

2 Breakout Rooms

- ✓ Individually search for two cyberattack incidents that occurred as a result of not following best security practices in cloud environments.
- ✓ Identify key details for each incident, including the type of cloud service involved, the nature of the security lapse (e.g., misconfigured storage, insufficient access controls), and the impact of the attack.

For each incident, write a short analysis (3–4 sentences) that covers:

- **What went wrong:** Describe the specific security best practices that were neglected.
- **Impact:** Outline the consequences of the cyberattack on the affected organization.
- **Lessons Learned:** Explain what could have been done to prevent the incident.

End of Lecture #10

Next Week, Project Presentation

15-20 min Presentation

5-10 min Q&A

THANK Y☺U

- Dawood Sajjadi

BCIT™