DON'T GET CAUGHT IN THE STORM: PROTECTING YOUR CLOUD ASSETS

Agenda

Introduction and Overview

- Course Description
- Learning Objectives
- Overview

IMR

- Identification
- Mitigation
- Response/Recovery

Case Studies

- Bank One
- Little Company, Big Leak
- Cybersecurity Solutions

Knowledge Check

Learning Objectives

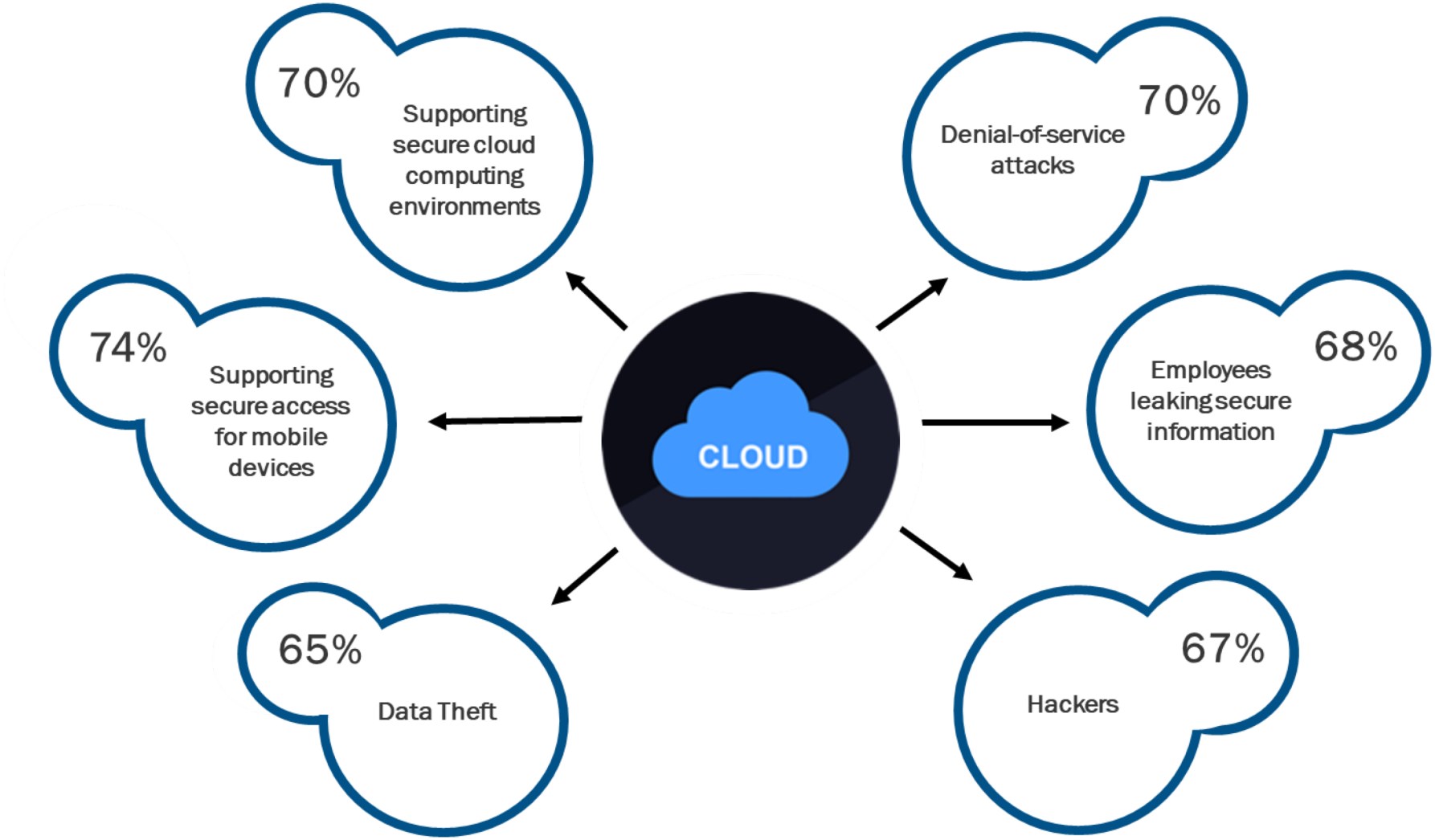
Terminal Objective

Understand the fundamentals of Cloud Based server attacks and the impact it can have on your organization

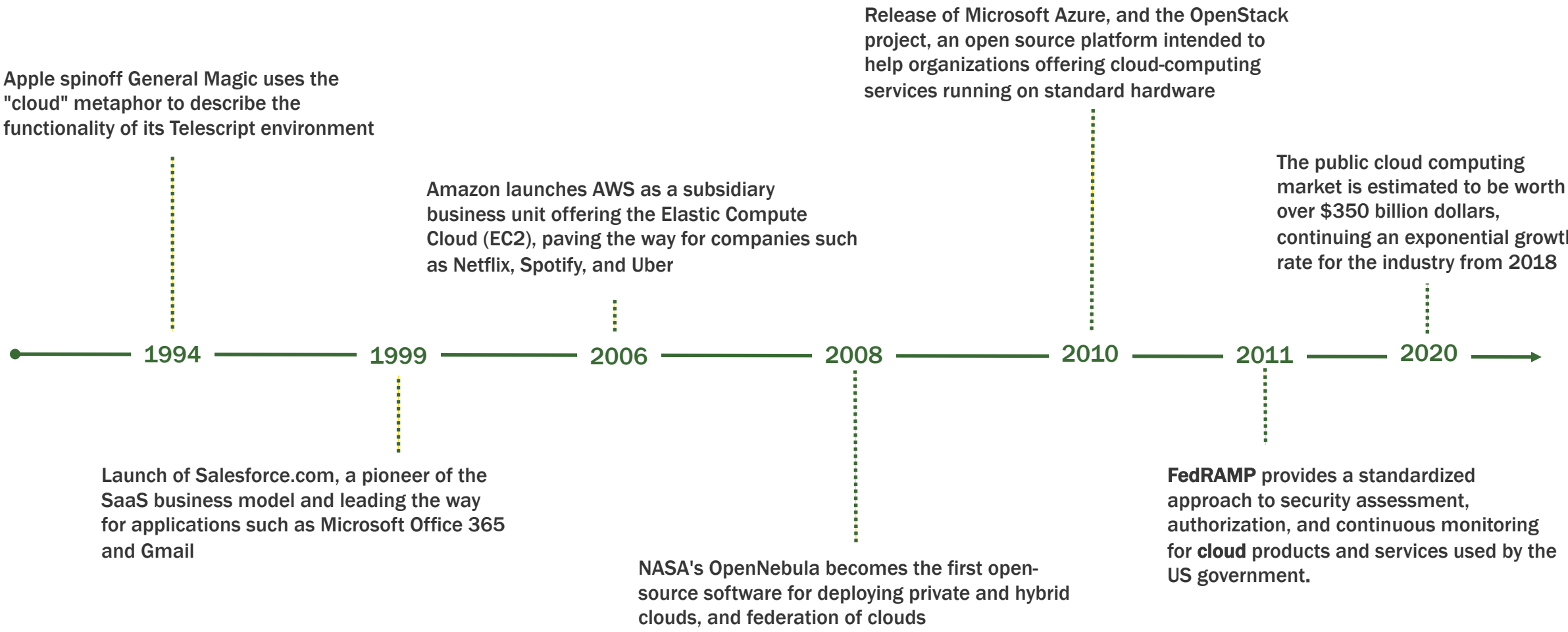
Enabling Objectives

- Define Cloud Based Server Attacks.
- Be able to identify signs of a Cloud attack.
- Learn mitigation steps of Cloud attacks.
- Understand how to recover from a Cloud attack.
- Understand impacts of Cloud attacks though case studies.

Percentage of cyber pros who say their agency is not completely prepared for the following:



Evolution of Cloud Computing



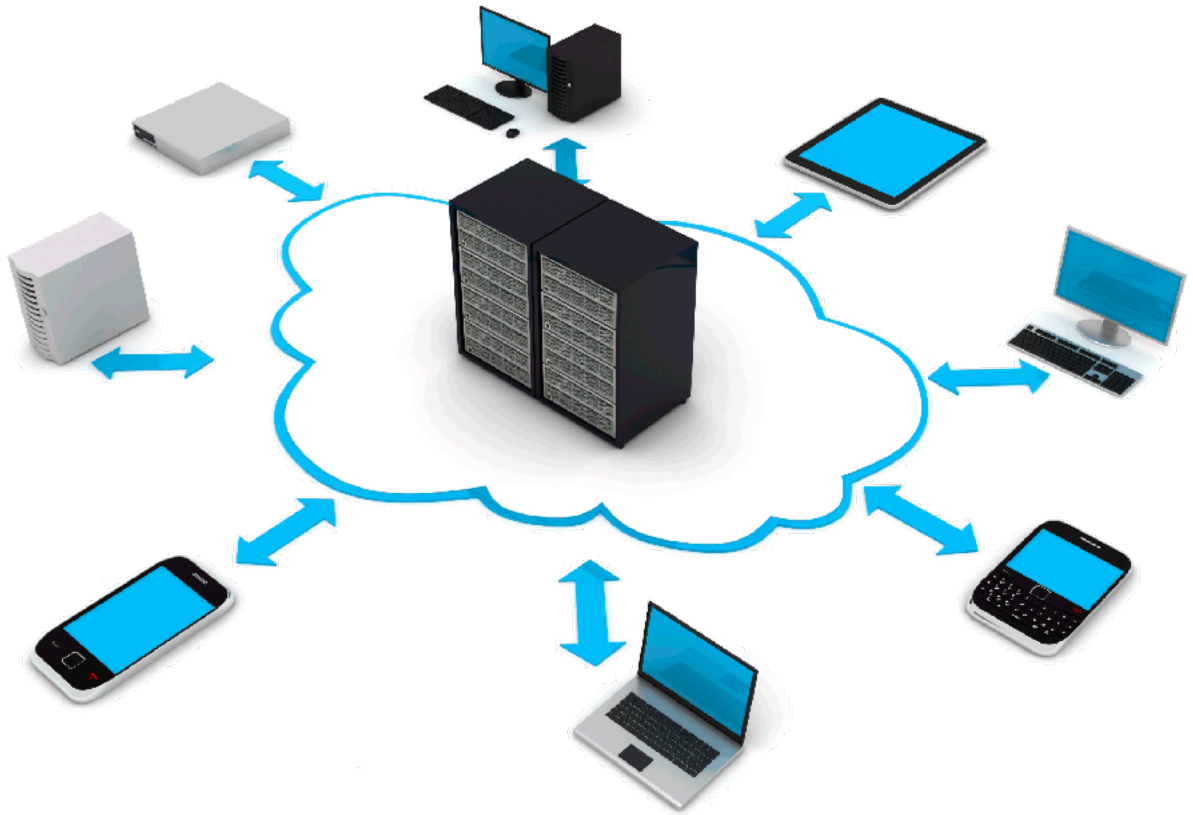
Overview: The Cloud

What is a Cloud Based Server?

A cloud server is a hosted computer server accessed by users over the internet. Cloud servers provide the same functions and support the same operating systems (OSes) and applications as traditional servers.

Why is Cloud Adoption Increasing?

- Cost effectiveness
  - Flexible
  - Scalable
  - Minimal Resource Management
- Globalization
- Ease of use

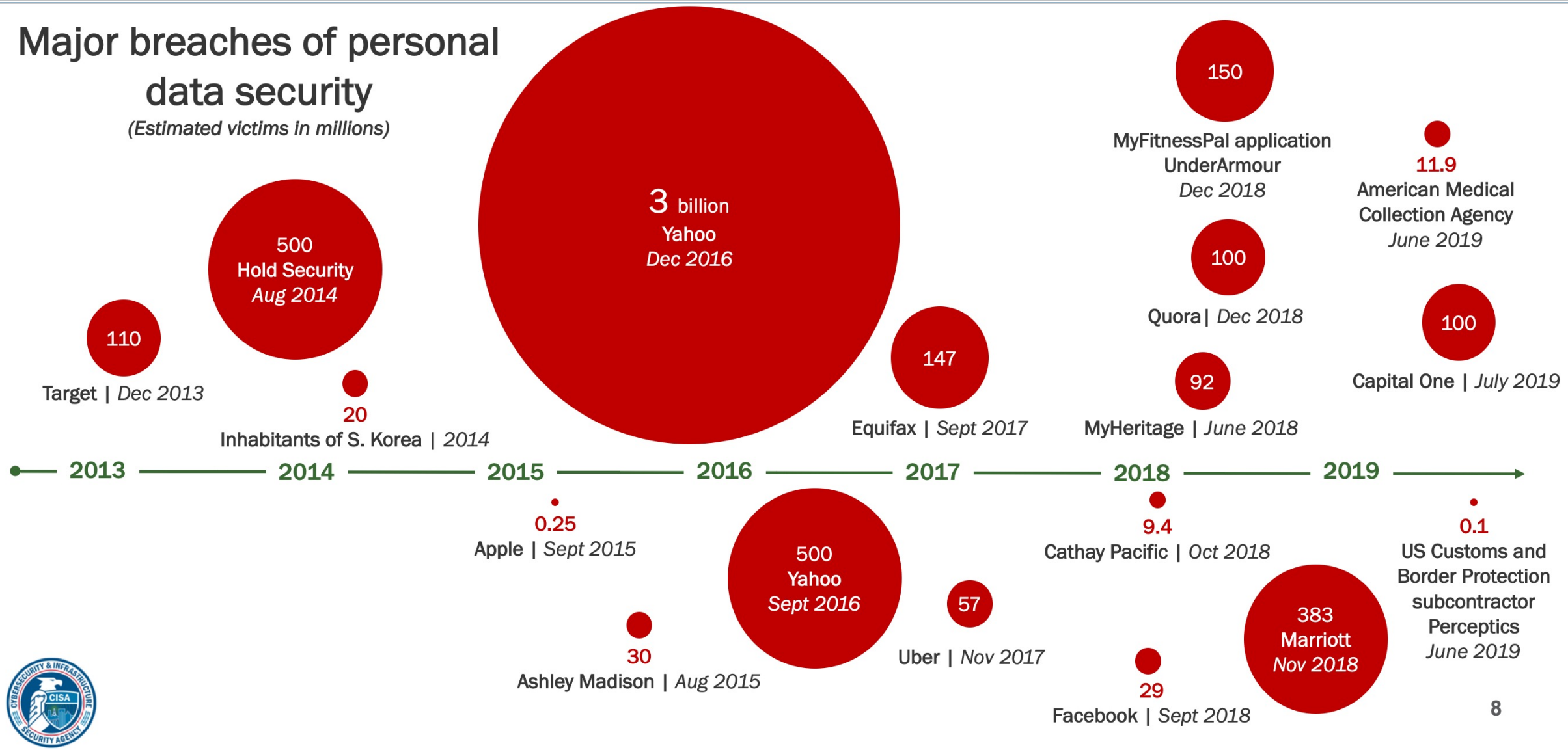


Overview: Cloud Attacks

Stages of a cloud-based server attack

- Hackers research a target system and look for any security vulnerabilities.
- An attack is staged for the targeted weakness.
- The attack is executed.

Who is Susceptible to Cloud Attacks?



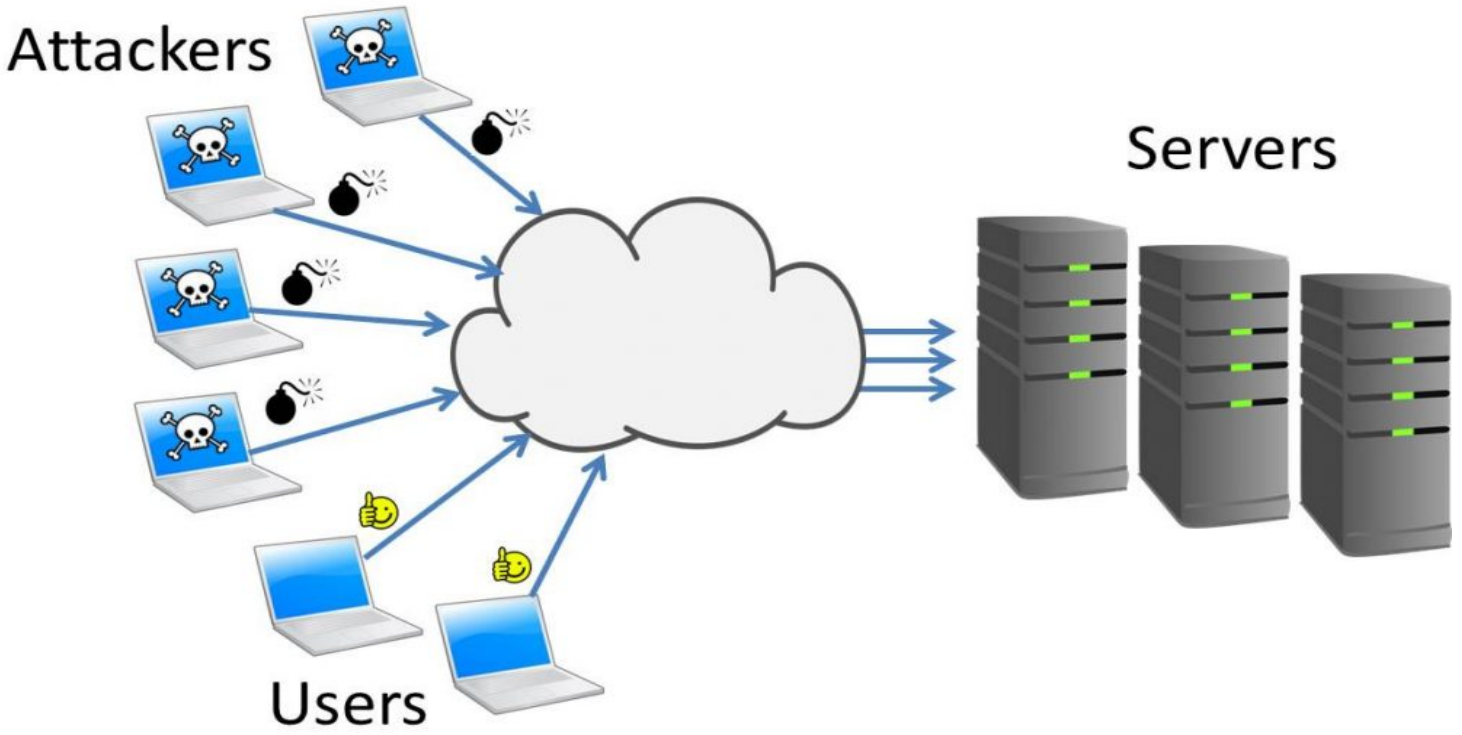
Source: Quora/Quest Diagnostics/Wired

How to Identify a Cloud Attack

Identify the Signs of a Cloud Attack

Indicators of a Cloud Attack:

- Excessive failed log-ins
- “Normal” user performing administrative tasks
- Analyze credential usage



Identify: Common Types of Attack

Denial of Service/ Distributed Denial of Service (DOS/DDOS) Attack:
Numerous compromised devices or systems (i.e. a botnet) target and overwhelm a system, preventing legitimate users from accessing it.

Insider Attack:
A security risk that originates from actors within the targeted organization.

Numerous threats:
Data breaches, Compromised Credentials, Account hijacking, Data Loss, Denial of Service Attacks

Cloud Attack Prevention and Mitigation

Best practices to prevent an attack:

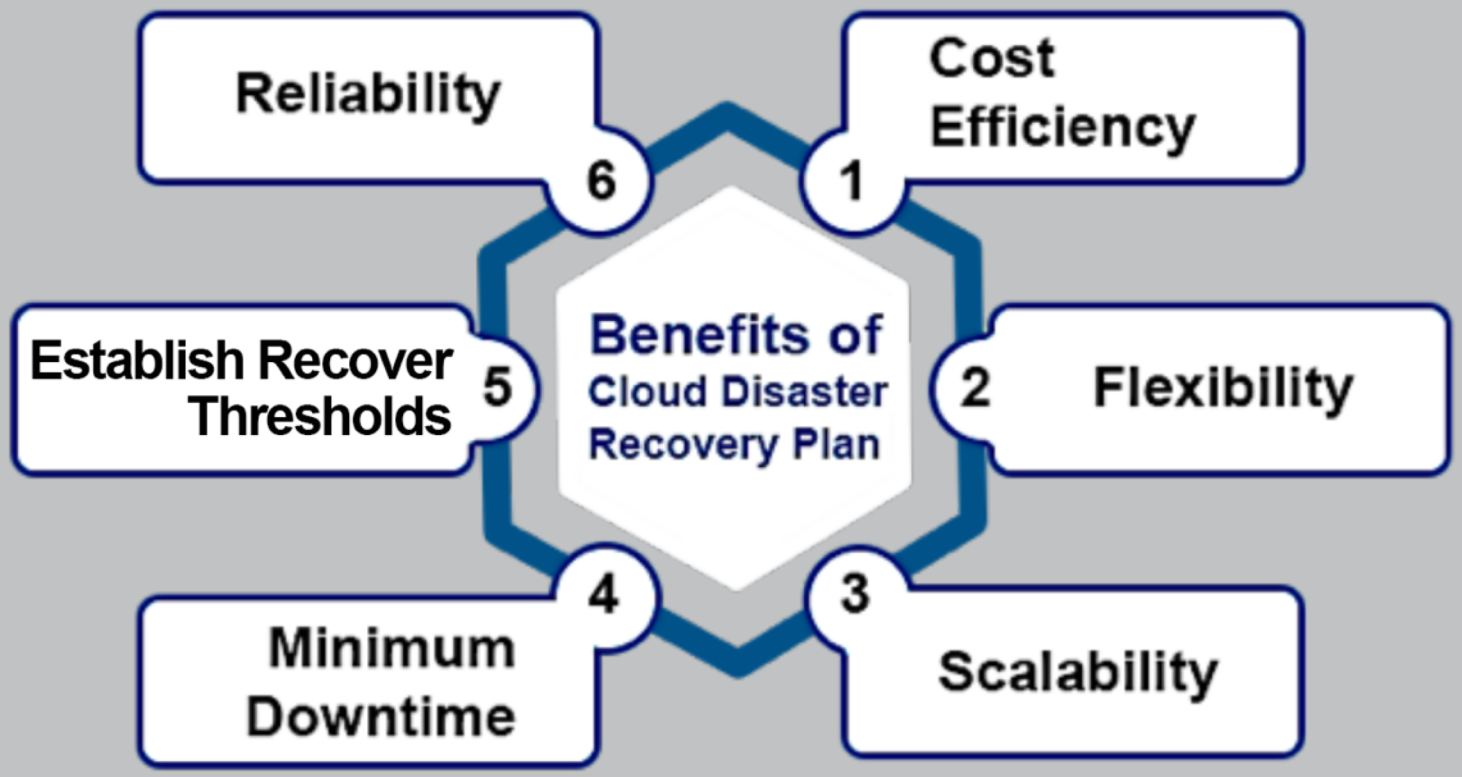
- **Access Control: Enforce Role-Based privileges:** Restrict access to users. Ensure privileges are role-based, and use session monitoring to record and monitor privileged access.
- **Monitoring:** Monitor all security network systems frequently.
- **Encryption:** Ensure cloud data is encrypted at rest and in transit.
- **Patching and maintenance:** Ensure third party cloud vendors update patches for any security vulnerabilities and include performance expectations in a service level agreement (SLA).

Recovery From A Cloud Attack

How to recover from a Cloud Attack:

- Ask for help! Contact CISA, the FBI, and law enforcement
- Identify what was compromised and potential damage
- Know your Service Level Agreements (SLA)
- Change passwords immediately on all accounts

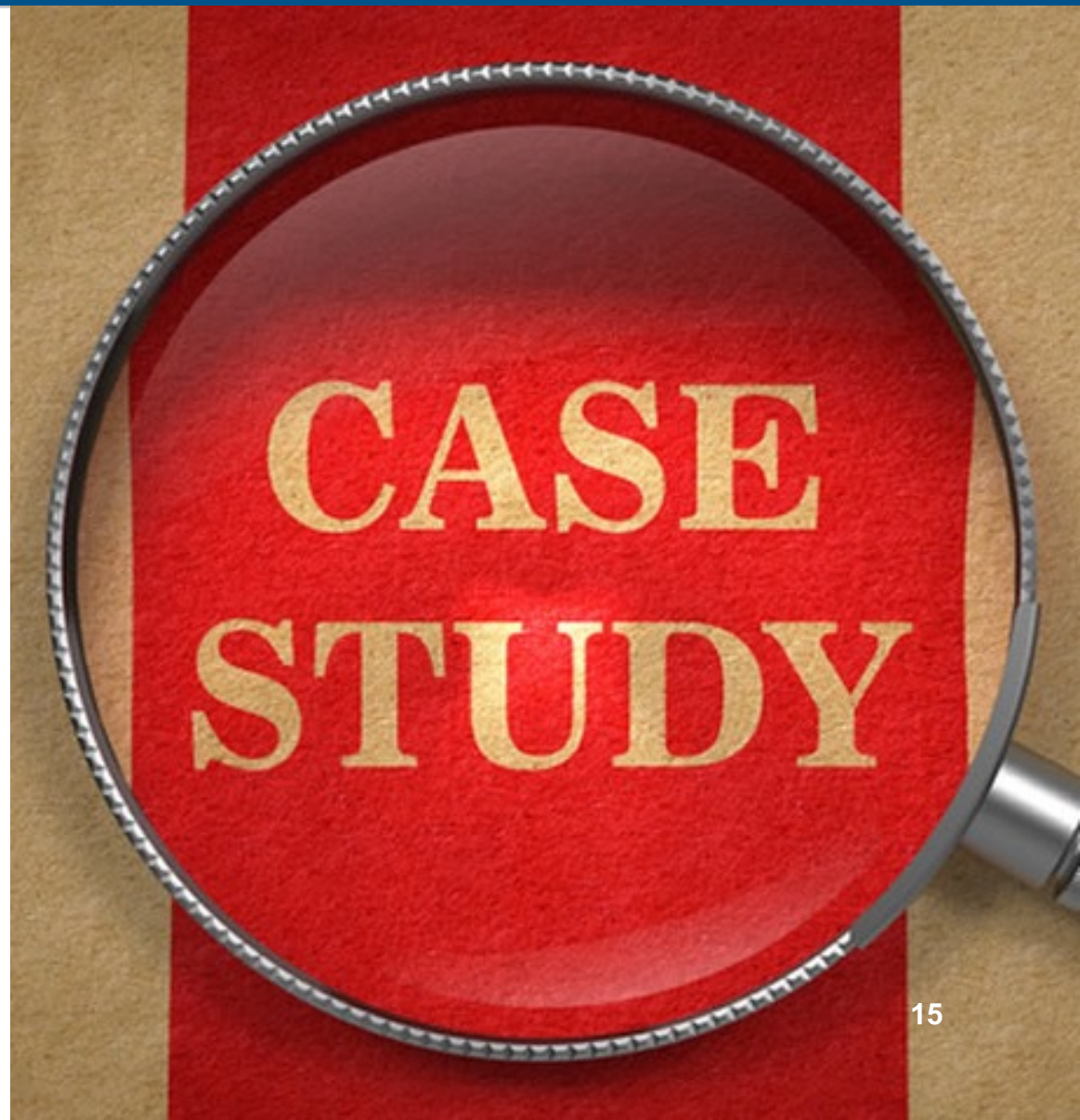
Recovery from a Cloud Attack



Cloud Case Studies

The following slides provide real life scenarios of companies that have suffered from Cloud-based Server Attacks.

- Bank One
- The Little Company that Leaked Big
- Managed Cybersecurity Solutions



Bank One

Scenario Overview

- In July of 2019 a well-known top 10 U.S. financial institution discovered that an individual gained unauthorized access and obtained personal information on more than 100 million customers in US and 6 million in Canada.
- A misconfigured firewall allowed the attacker to exfiltrate over 106 million credit card applications including customer PII.

Bank One

What was the threat and attack vector?

A former Systems Engineer for the Cloud Service Provider (CSP) hacked a misconfigured firewall and stole data from **over 100 million** credit card applications.

What vulnerabilities were exploited?

The attacker used a well-known method called "**Server-Side Request Forgery**" (SSRF), in which a server can be manipulated into running commands that it should not have permission to run.

Bank One

What was the impact of the attack on the organization?

- 100+ million in US and 6 million in Canada had data stolen.
  - Bank account numbers
  - Social Security numbers
  - Credit scores
  - Names and addresses
  - Phone numbers, birthdays, and emails
  - Self-reported income information
- Partial data was stolen on transactions occurring during 23 days in 2016, 2017, and 2018.

Bank One

How was this attack Identified?

- The attacker posted code to GitHub showing how the attack was carried out.
- Bank One received an anonymous tip, leading them to contact the FBI and begin an investigation.

How was the attack Mitigated?

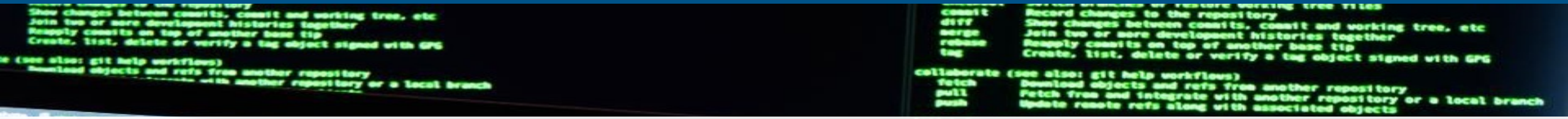
- Notified all US and Canadian customers affected.
- Offered free credit monitoring and identity protection.
- Repaired the firewall misconfiguration that permitted the hacker to access the server.

Bank One

How did the organization Recover?

- Fixed the misconfigured firewall, disabled privileged user credentials, and collaborated with the FBI.
- Encouraged affected customers to enroll in account alerts.
- FBI captured the individual responsible for the breach.
- Implemented sophisticated fraud systems to protect customers from unauthorized actions.
- Encouraged all customers to monitor credit card accounts for suspicious activity.

The Little Company that Leaked Big



Scenario Overview

- A small but major data company based in Florida leaked the data of 340 million individuals, according to the security researcher who discovered the breach.
- A company you've likely never heard of allegedly exposed very personal data on "pretty much every U.S. citizen."

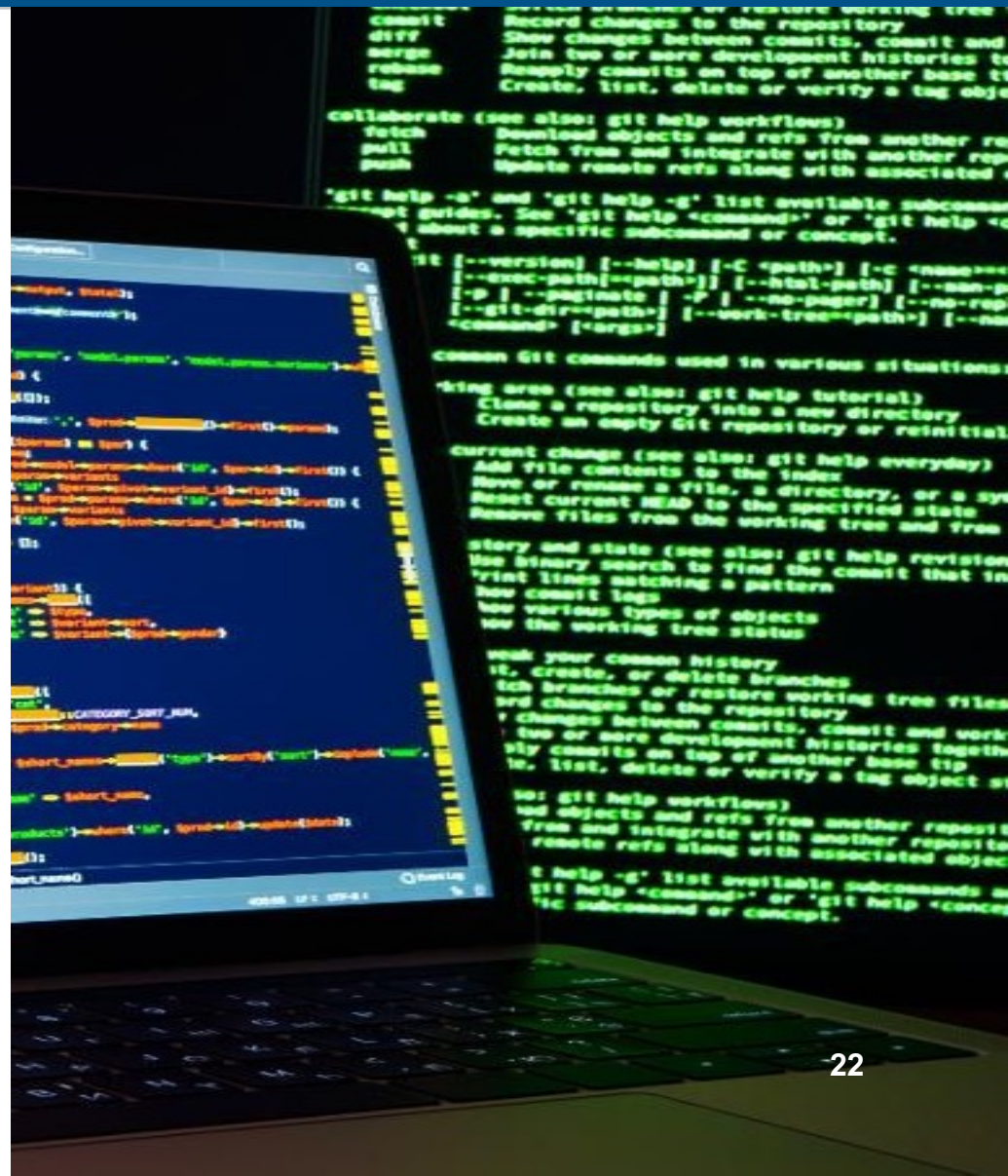
The Little Company that Leaked Big

Cause of the Leak:

A Security researcher searched for visible databases on publicly accessible servers with American IP addresses and found the database, unprotected by any firewall.

Impact on the company:

- Loss of business partners
- Class action lawsuit
- Loss of partnerships
- Loss of the business



The Little Company that Leaked Big

How was this attack identified?

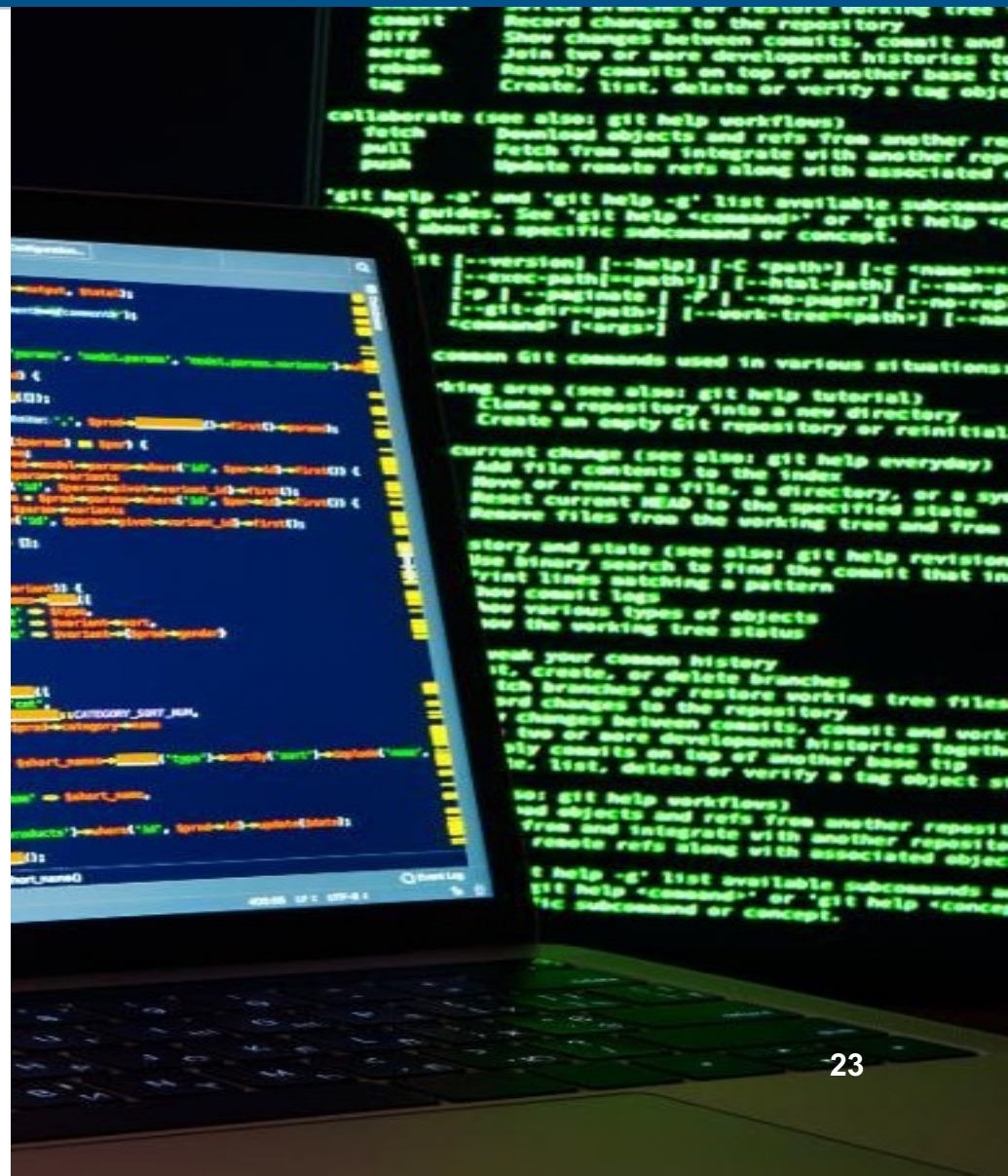
The security researcher found the exposed database containing almost 340 million individual records and notified the company and the FBI.

How was the attack mitigated?

- The leak was fixed quickly upon discovery, but the company quickly lost business and business partners.

How did the organization recover?

- The company went out of business.



Managed Cybersecurity Solutions

Scenario Overview:

- On August 20, 2019 a leading provider of Internet firewall services alerted customers that a recent data breach exposed email addresses, scrambled passwords, API keys, and SSL certificates for a subset of its firewall users.
- An accidental exposure of a database snapshot allowed attackers to access it, leaking emails, hashed passwords, and security credential information.

Managed Cybersecurity Solutions

What was the threat and attack vector?

- A compromised compute instance leaked an AWS API key, allowing attackers to access a database snapshot.
- A misconfiguration of an Amazon Web Services (AWS) cloud instance allowed hackers to exfiltrate information on customers using MCS's Cloud Web Application Firewall (WAF) product.

Managed Cybersecurity Solutions

What vulnerabilities were exploited to accomplish the attack?

Misuse of an administrative API key in one of the company's AWS accounts in October 2018 led to exposure of a database snapshot containing emails and hashed passwords.

What was the impact of the attack on the organization?

- Attackers could whitelist themselves to circumvent the WAF.
- Attackers could intercept, view or modify traffic destined for a client website.
- Or divert all traffic for that site to or through an attacker-controlled website.

Managed Cybersecurity Solutions

How was the attack Identified?

- A third party contacted the company, provided a copy of the stolen data, and requested a bug bounty.
- In October 2018, the intruder downloaded a copy of the database snapshot uploaded on the AWS environment.

How was the attack Mitigated?

- Changed 13,000 user account passwords for Cloud WAF.
- Enabled Single Sign On and two-factor authentication.
- Reset 1,400 API keys.
- Rotated 13,500 new SSL certificates.

Managed Cybersecurity Solutions

How did the organization Recover?

- Repaired the vulnerability and promptly reached out to FBI.
- Forced password rotations and 90-day expiration policies.
- Enforced SSO and multi-factor authentication in AWS management console.
- Incorporated lessons learned into security programming.

Knowledge Check

Knowledge Check

A cloud-based server is the primary storage hardware/component within a computing device, and it's used to store, retrieve and organize data.

- ○ True
- ○ False

Knowledge Check

A cloud-based server is the primary storage hardware/component within a computing device, and it's used to store, retrieve and organize data.

- ○ False

Knowledge Check

_____ is a security risk that originates from within the organization.

- DOS Attack
- Side Channel Attack
- Cross Cloud Attack
- Insider Attack

Knowledge Check

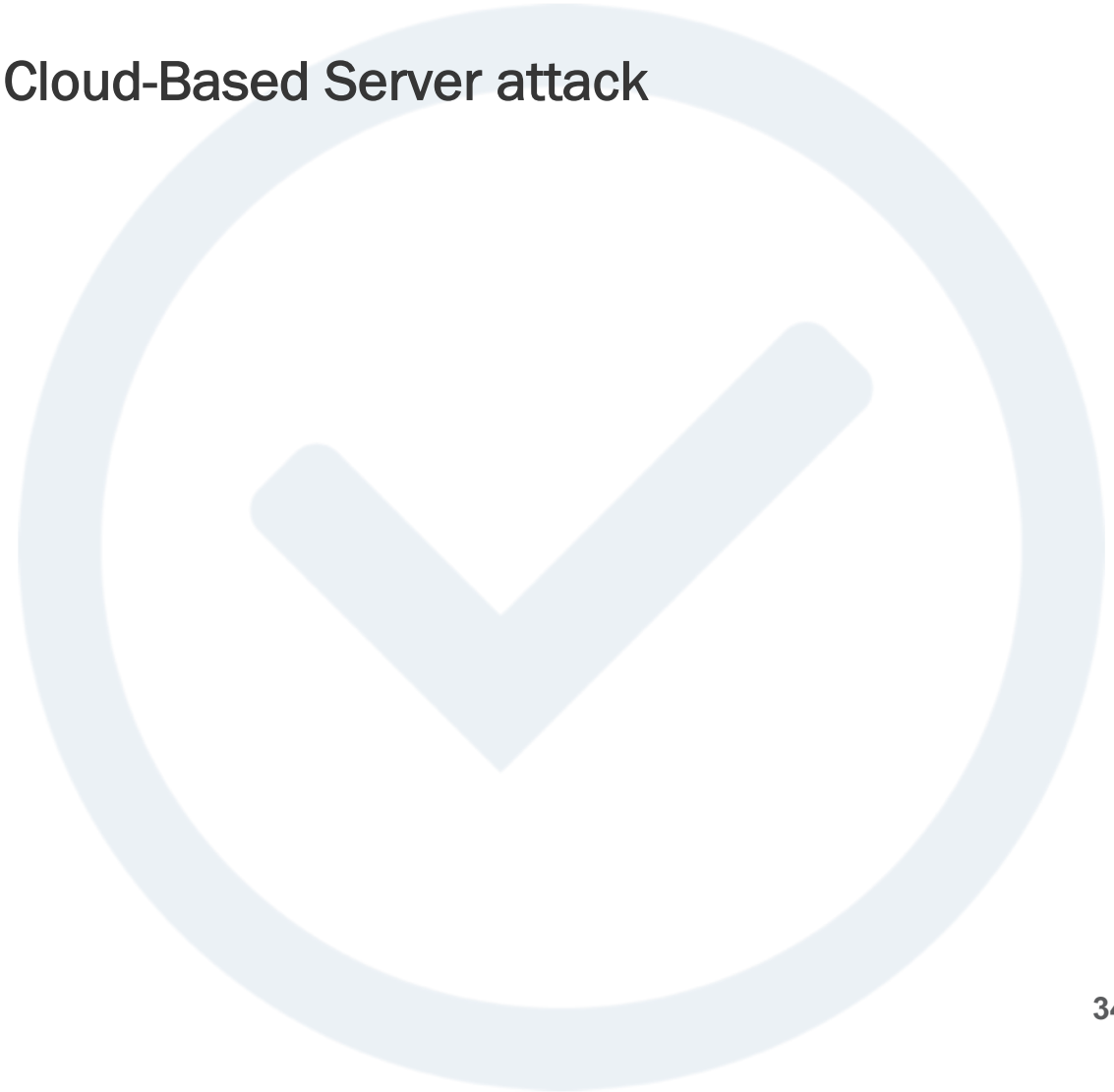
_____ is a security risk that originates from within the organization.

- Insider Attack

Knowledge Check

Excessive failed log-ins is a key indicator of a Cloud-Based Server attack

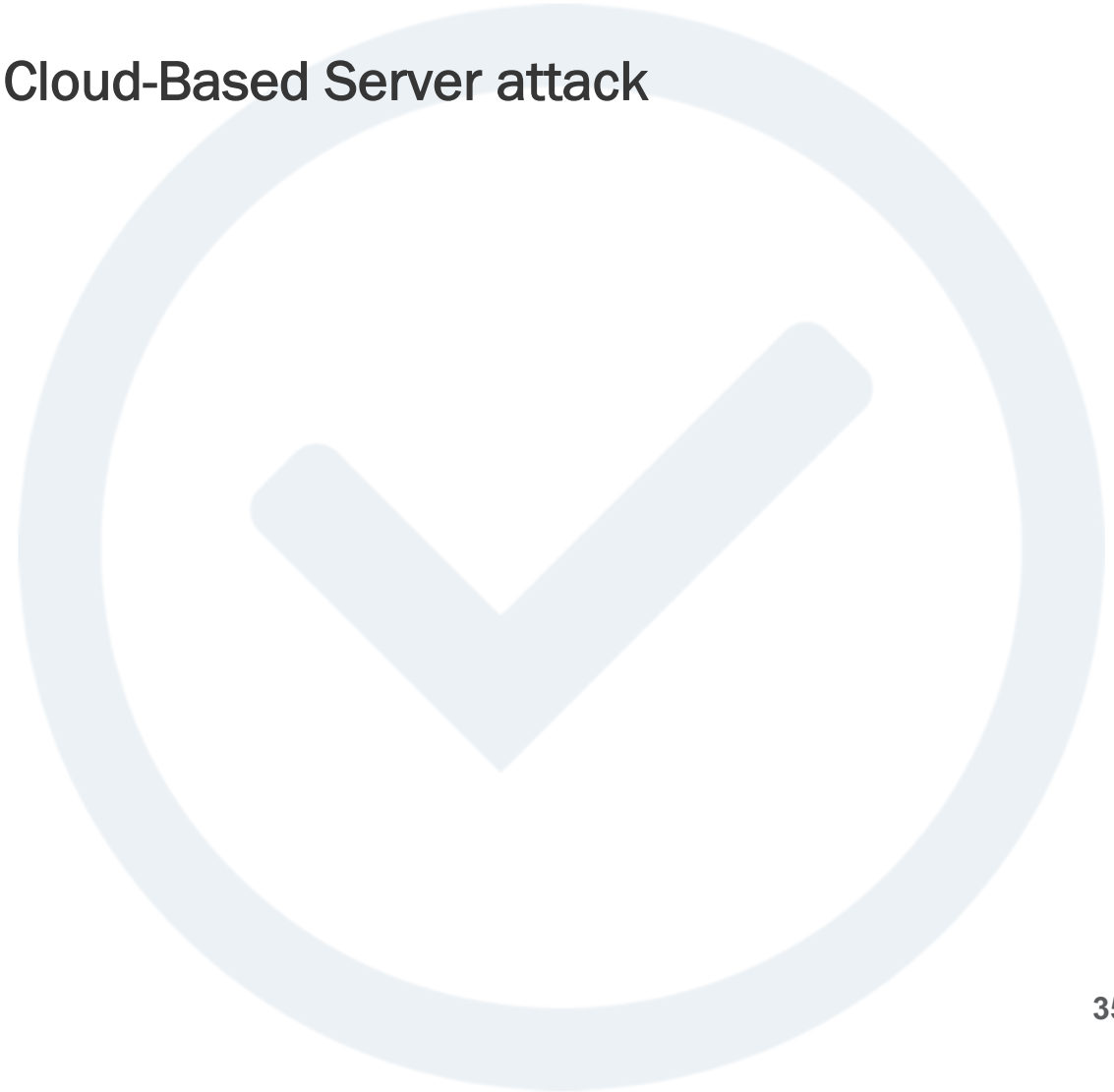
- ❍ True
- ❍ False



Knowledge Check

Excessive failed log-ins is a key indicator of a Cloud-Based Server attack

- ○ True



Knowledge Check

The NICE Framework is a blueprint to categorize, organize, and describe cybersecurity work into categories, specialty areas, work roles tasks, and Knowledge, Skills and Abilities (KSA)

- ○ True
- ○ False

Knowledge Check

The NICE Framework is a blueprint to categorize, organize, and describe cybersecurity work into categories, specialty areas, work roles tasks, and Knowledge, Skills and Abilities (KSA)

- ○ True

Knowledge Check

Which statement is true about a cloud computing environment?

- ❍ It cannot be used to host location based applications.
- ❍ It enables users to access systems regardless of their location.
- ❍ It introduces latency as the servers are geographically dispersed.
- ❍ It can improve a web server response time by having servers closer to the end user.

Knowledge Check

Which statement is true about a cloud computing environment?

- ❍ It enables users to access systems regardless of their location.

Knowledge Check

What is cloud computing replacing?

- Corporate data centers
- Expensive personal computer hardware
- Expensive software upgrades
- All of the above

Knowledge Check

What is cloud computing replacing?

- ○ All of the above

Knowledge Check

Security in a Cloud based environment protects

- Data
- Applications
- Infrastructure
- All the Above

Knowledge Check

Security in a Cloud based environment protects

- ○ All the Above

Knowledge Check

What are two important benefits of using cloud computing? (Choose two.)

- ❍ Mobility
- ❍ Deployment of single tenant application.
- ❍ Enhanced Web V2.0 interfaces for user interactions
- ❍ Lower total cost of ownership and improved asset utilization.
- ❍ Provides better availability than a standard computing environment.

Knowledge Check

What are two important benefits of using cloud computing? (Choose two.)

- ❍ Mobility
- ❍ Lower total cost of ownership and improved asset utilization.

Knowledge Check

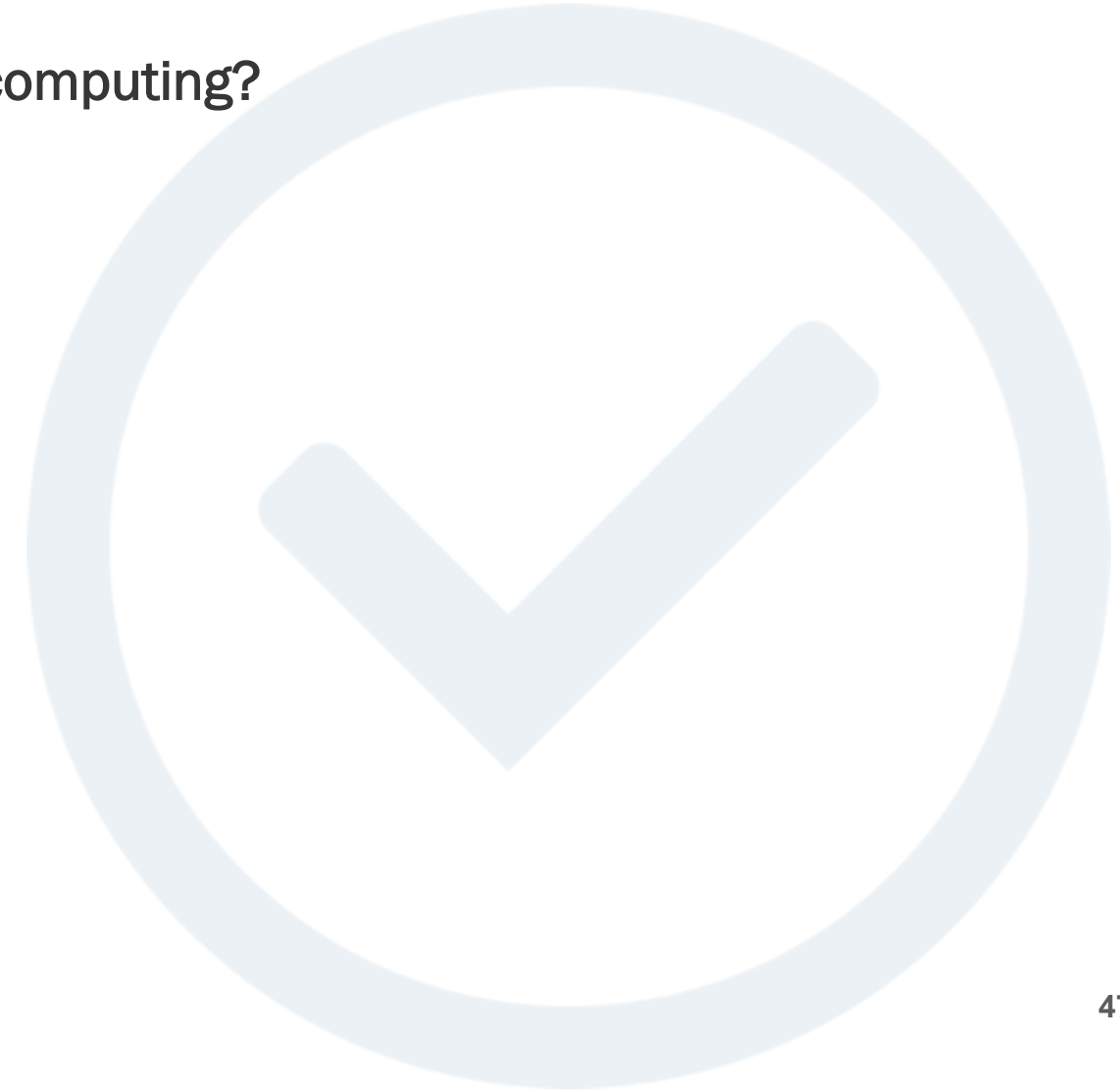
What is the benefit to virtualization in cloud computing?

- ❍ It removes operating system inefficiencies.
- ❍ It improves the performance of web applications.
- ❍ It optimizes the utilization of computing resources.
- ❍ It adds extra load to the underlying physical infrastructure and has no role in cloud computing.

Knowledge Check

What is the benefit to virtualization in cloud computing?

- It optimizes the utilization of computing resources.



Knowledge Check

What are some best practices to mitigate an attack on an organization's Cloud – Based Server?

- Monitoring
- Patching and Maintenance
- Minimize usage on the Cloud-Based Server
- Encryption

Knowledge Check

What are some best practices to mitigate an attack on an organization's Cloud – Based Server?

- Monitoring
- Patching and Maintenance
- Encryption

Key Takeaways

- **Recognize CBS Attacks**
  - Excessive failed log-ins
  - Unexplained credential usage
  - Normal users performing admin tasks

IDENTIFY

- **Prevention Tips**
  - Access control
  - Authentication
  - Monitor
  - Encryption
  - Patching

MITIGATE

- **Find Solution**
  - Contact CISA
  - Identify damage
  - Change passwords
  - Know your Service Level Agreement (SLA)

RECOVER

Additional Cloud Based Server Resources

- NSA: Mitigating Cloud Vulnerabilities
- CISA: Publications
- US-CERT: Common Risks of Using Business Apps in the Cloud

CISA and NDU Present:
Professors in Practice Series

Examining the World of the Authorizing Official

Risk Management Framework for Leaders (feat. Professor Mark Duke)

Online: July 10, 2020 11:00 a.m. – 12:00 p.m.

FedRAMP – A Leader's Dashboard for Compliance (feat. Professor George Trawick)

Online: July 17, 2020 11:00 a.m. – 12:00 p.m.

Cloud Security - What Leaders Need to Know (feat. Professor Robert Richardson)

Online: July 24, 2020 11:00 a.m. – 12:00 p.m.

A Leader's Approach to Assessment and Authorization (A&A) (feat. Professor Mark Duke)

Online: July 31, 2020 11:00 a.m. – 12:00 p.m.

Sign Up: https://www.us-cert.gov/cdm/training

CISA
CYBER+INFRASTRUCTURE


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY