

# Network Threats and Attacks

---



**Kevin Henry**

CISM CISSP CCSP

[kevin@kmhenrymanagement.com](mailto:kevin@kmhenrymanagement.com)



# Network Security for the CC<sup>SM</sup> Certification

## **Agenda:**

**Computer  
Networking**

**Network Threats  
and Attacks**

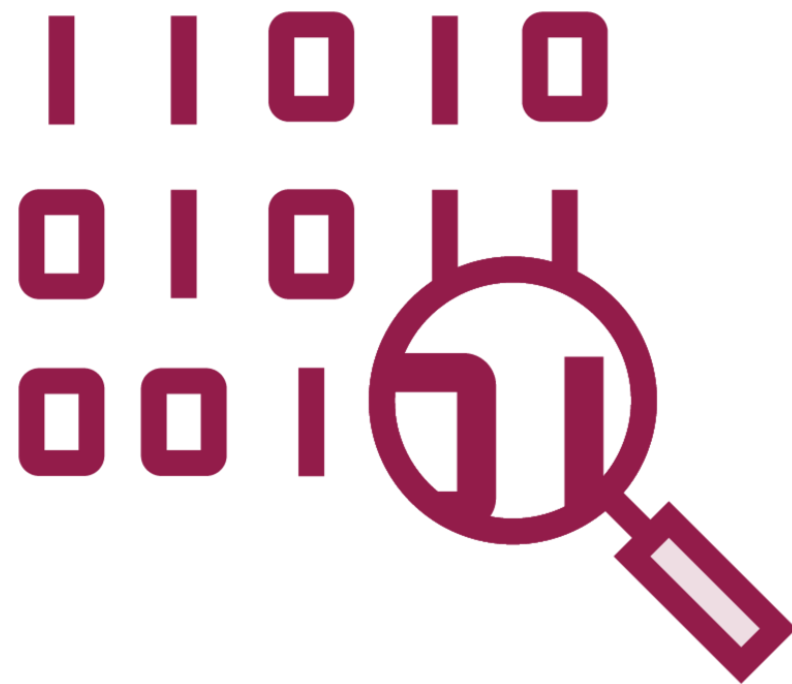
**Network  
Infrastructure**



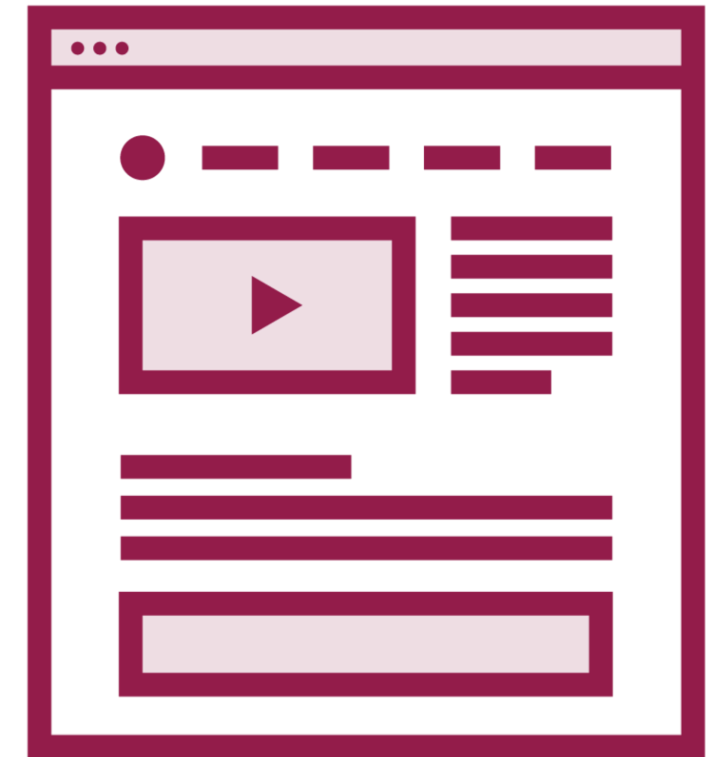
# Threat Intelligence



**Commercial feeds**



**Open Source  
Intelligence  
(OSINT) feeds**



**Blogs**

# Threat Hunting

**Monitoring of traffic**

**Analysis of attack signatures**

**Similar attack methods**

**Similar targets**



# DDoS Mitigation

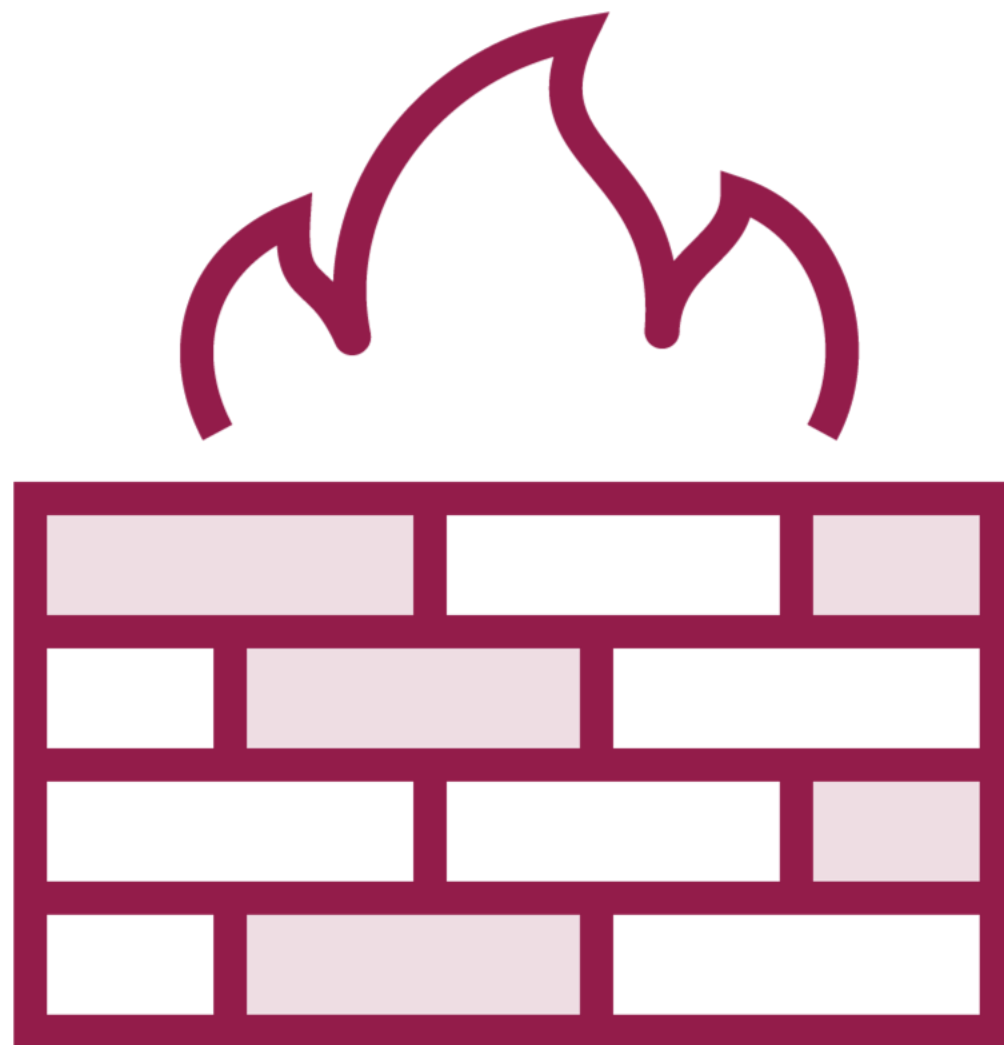


**Attack deflection**  
**Anti-spam organization**



**Absorb attack traffic**

# Firewalls



## Gateway between networks

- Control inbound and outbound traffic
  - Egress Monitoring
- Whitelisting
- Blacklisting
- Correct placement





# Firewall Operations

## Configuration

## Rules

- Change control

## Monitoring

- Challenge of encryption
- Virtual Private Networks

## Training of staff



# IDS and IPS

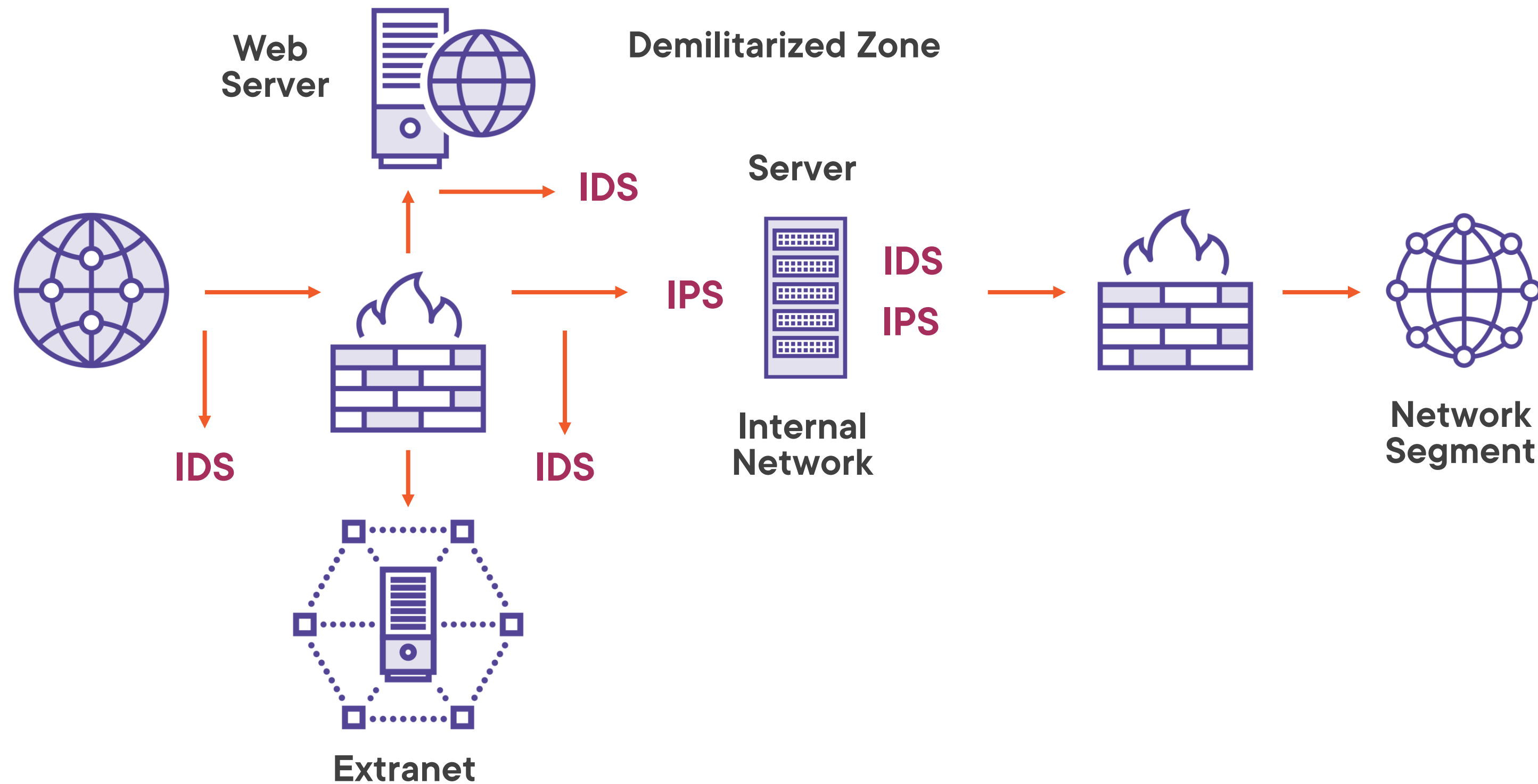
**Intrusion Detection and  
Prevention Systems**

**Misuse detection**

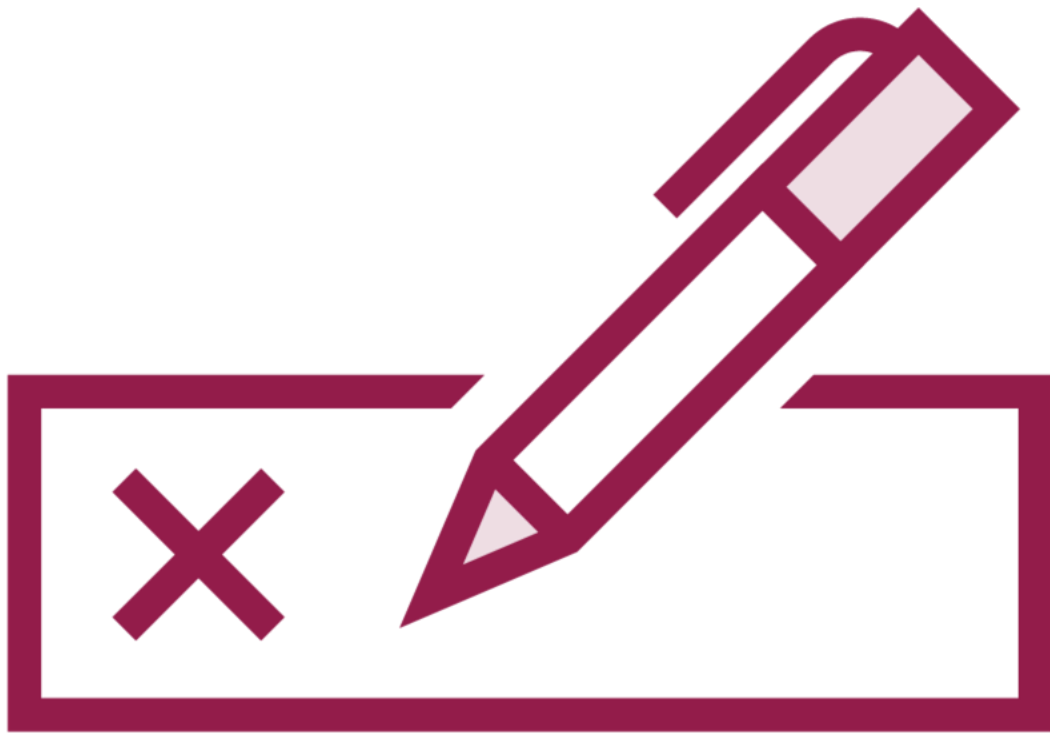
**Part of layered defense**



# Firewall and IDS/IPS Placement



# IDS and IPS Operations



## Pattern Matching and Signature based

### Anomaly detection

- Protocol
- Traffic
- Statistical
- Heuristic

# Malware

---



# Malware

**Software written to do harm**  
**Does not include bugs or flaws**

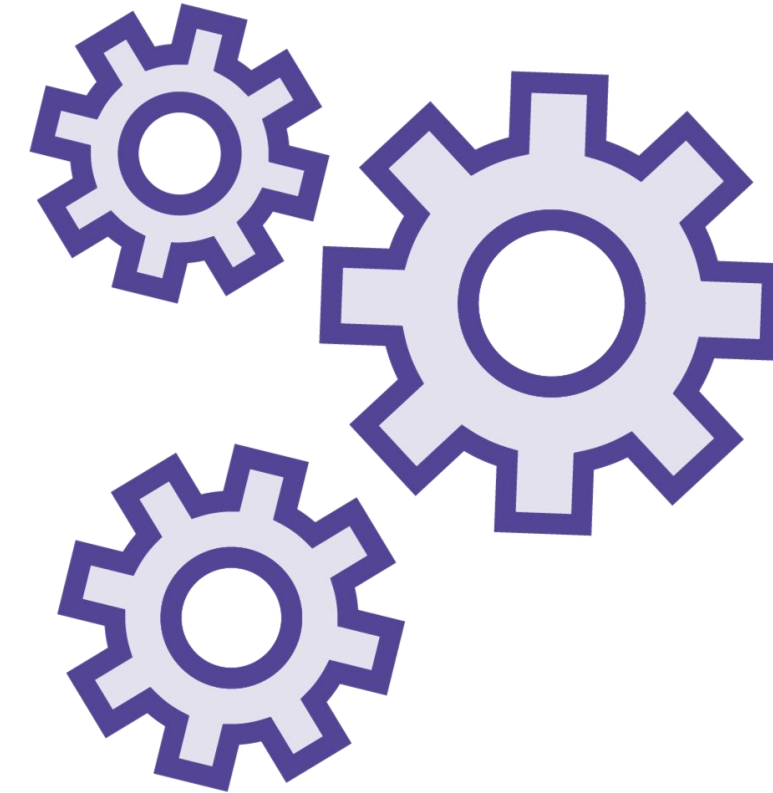
**Evolution of malware and  
malware authors**



# Anti-Malware



**Awareness training**



**Anti-malware tools**  
**Signatures**  
**Monitoring**

# Sandboxing

## Isolation

## Isolated systems

- Forensics
- Malware analysis

## Virtual environments



# Honeypots and Honeynets

**Target of Opportunity**

**Learn attack behaviors**

**Design better defenses**

**Traffic analysis**

**Side channel**



# High Layer Attacks

**Malware**

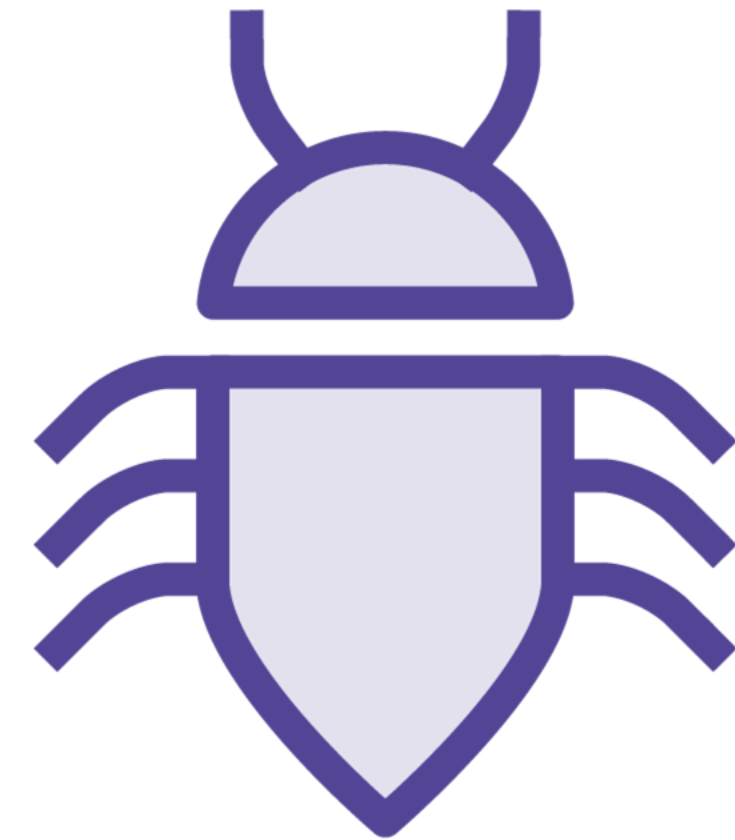
**Spam**

**Man-in-the-middle**

**Software flaws**

**Session management**

**Timeouts**



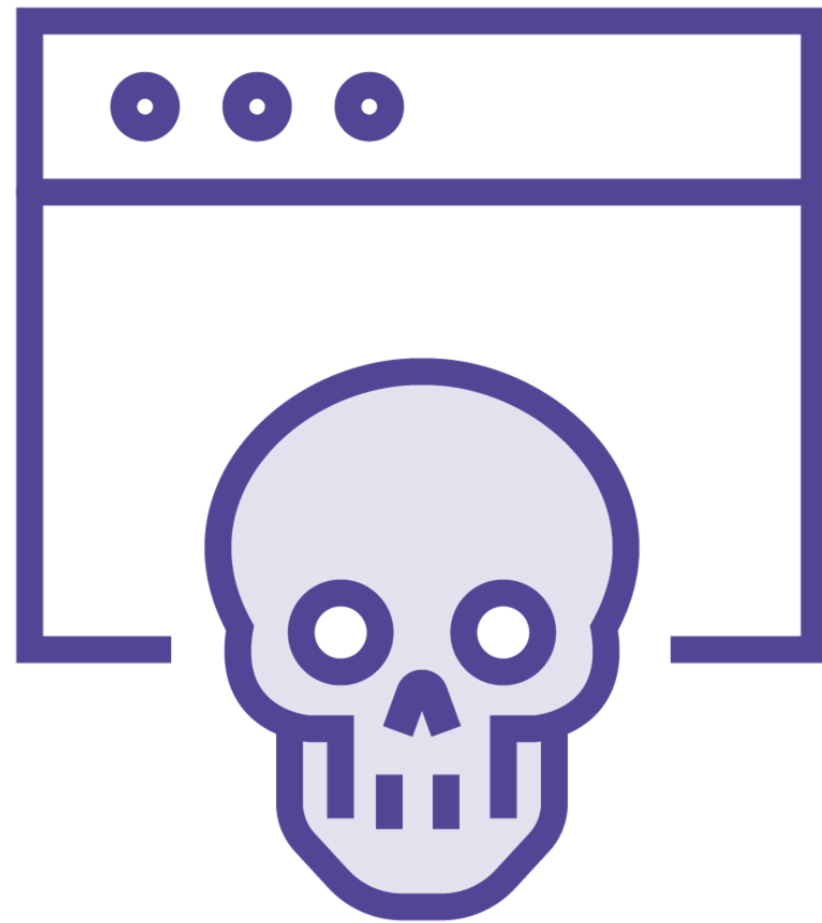
# Transport Layer Attacks



## Flooding

- SYN flood
- UDP Flood
- TCP sequence
- MITM

# Network Layer Attacks



## IP Spoofing

### ICMP

- Ping of death
- Flood – SMURF



# Data Link and Physical Layer Attacks



**Jamming**

**Sniffing**

**Cable damage**

- Theft

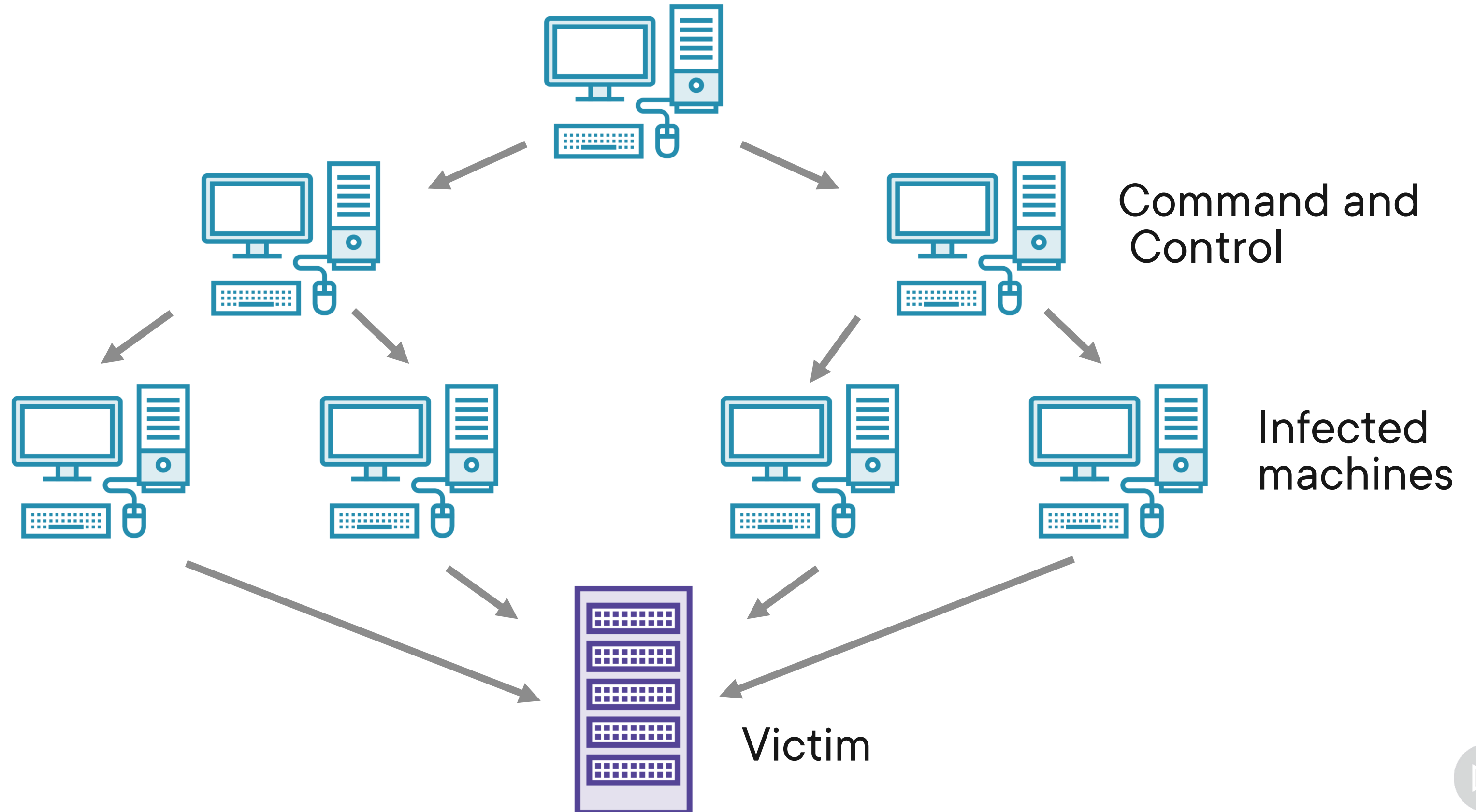


# Botnets

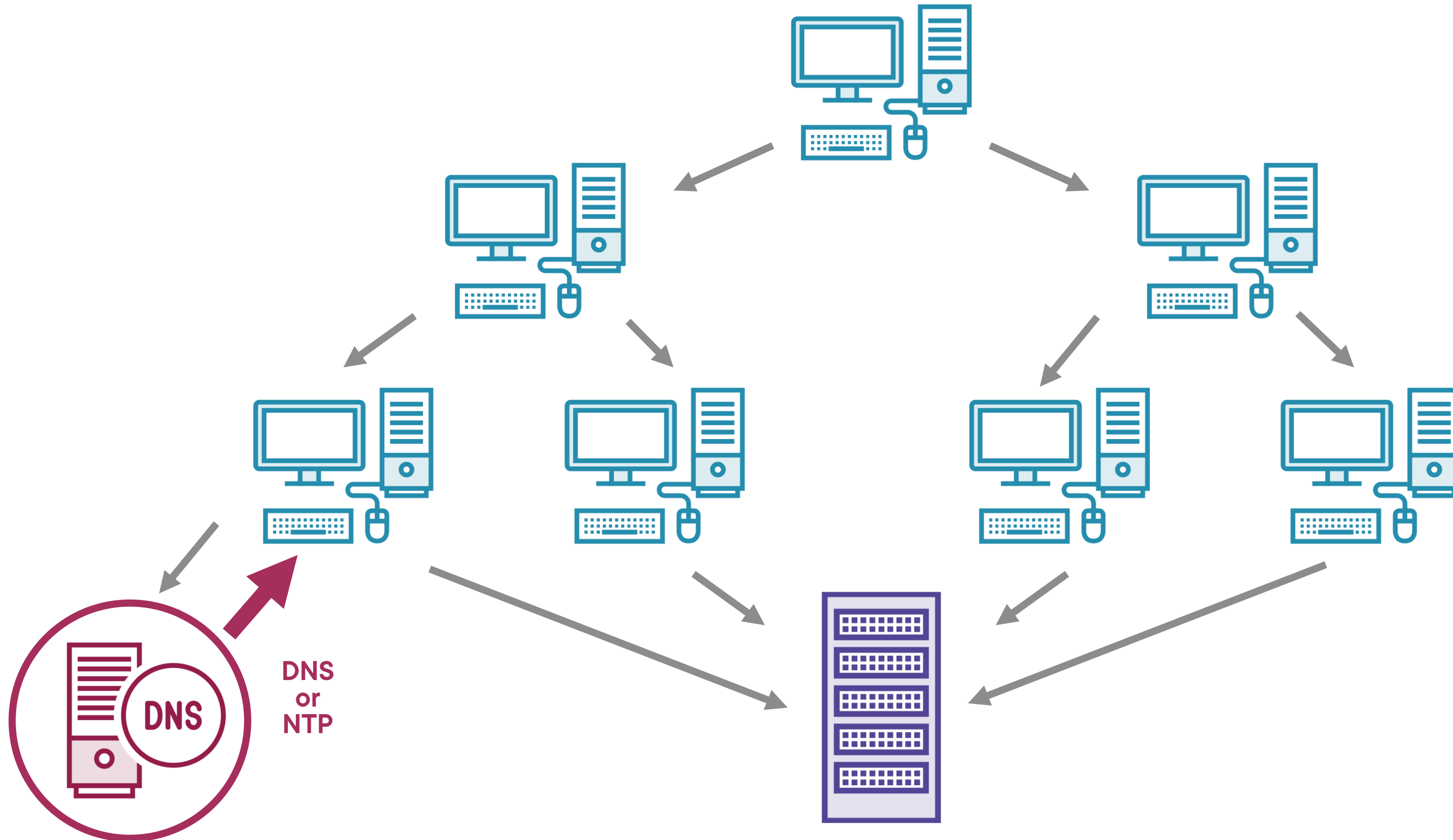
---



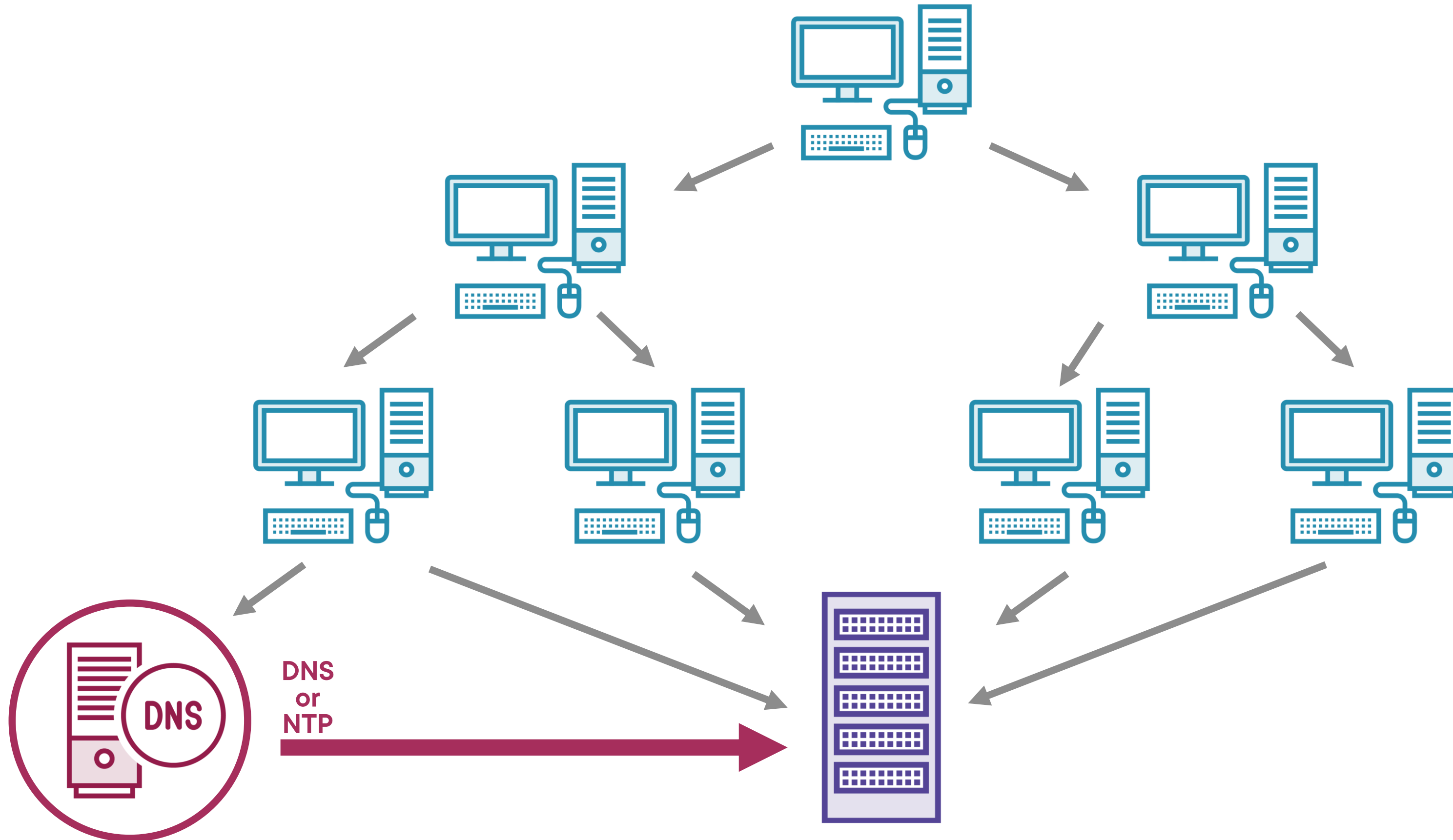
# Botnets



# Botnets



# Botnets



# Example of an Attack

---





# Large retail organization

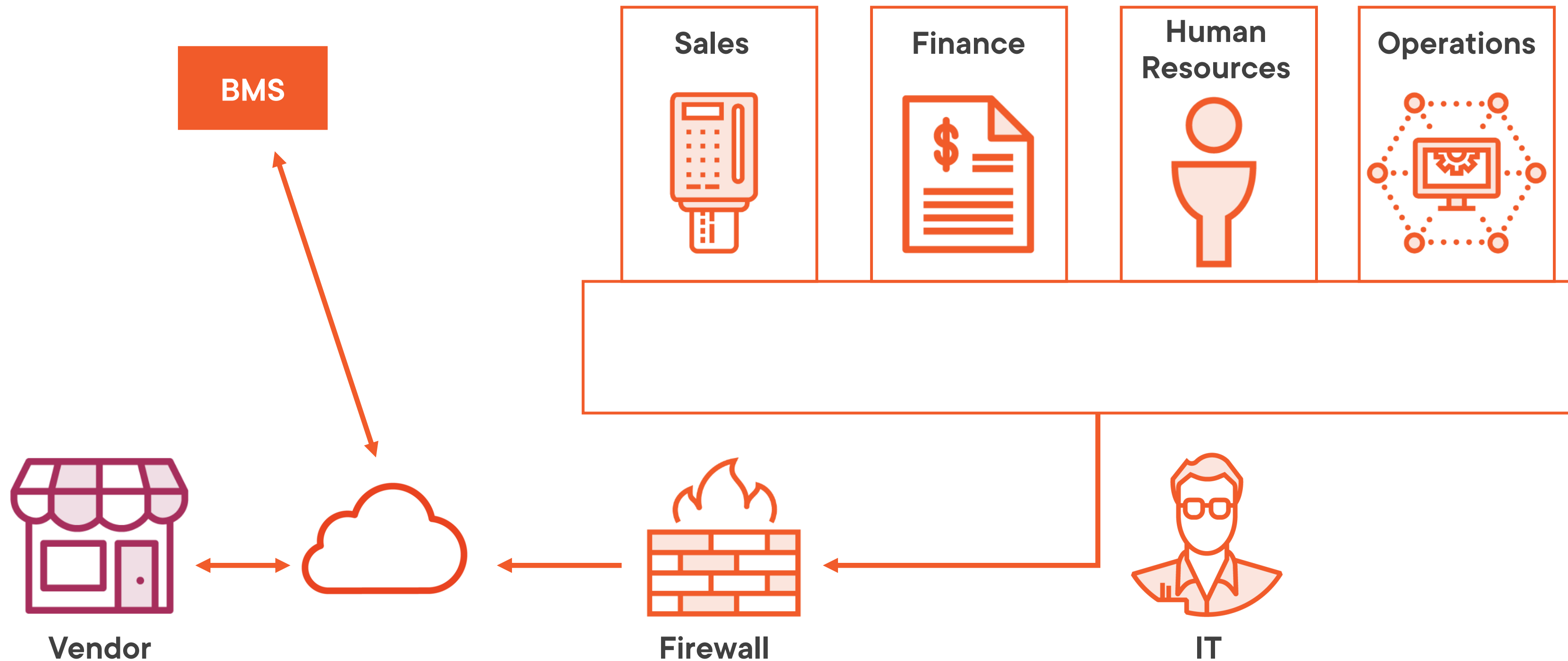
Loss of millions of credit cards



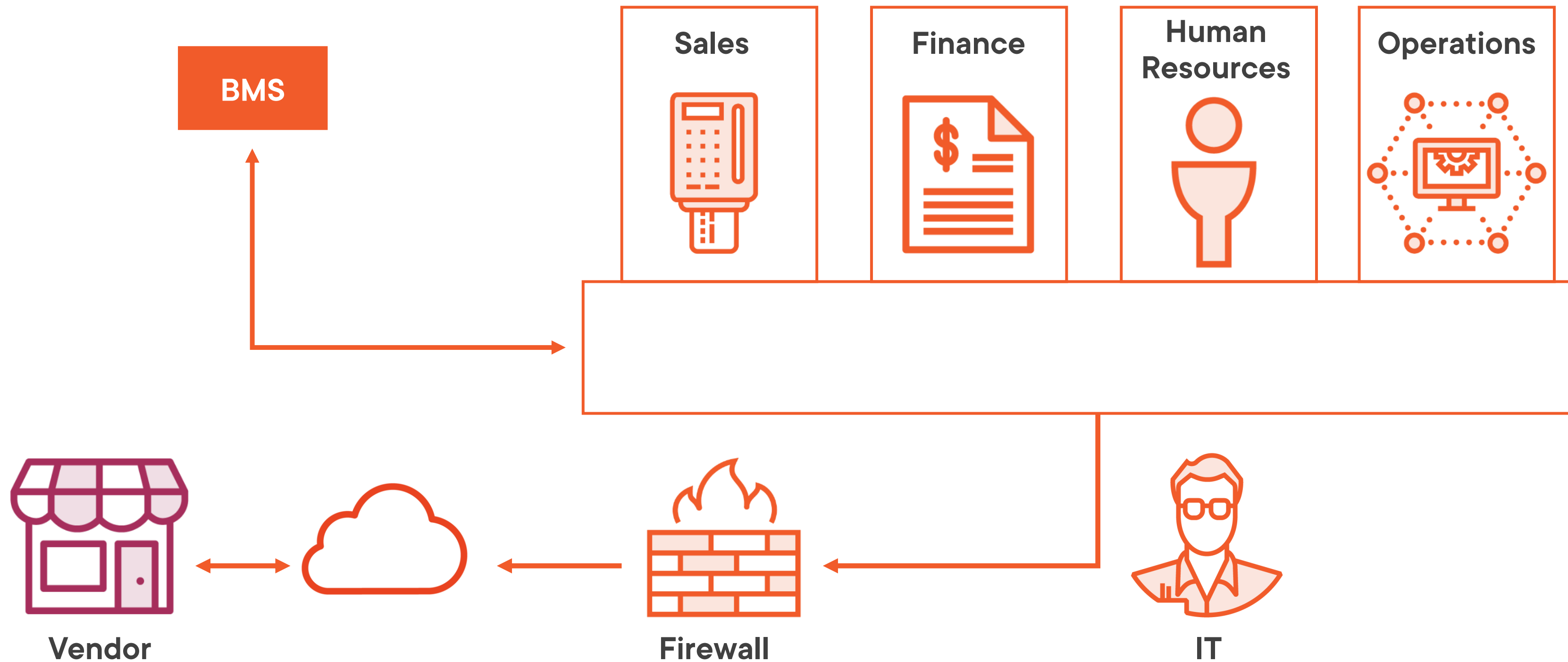
# The Way It Happened



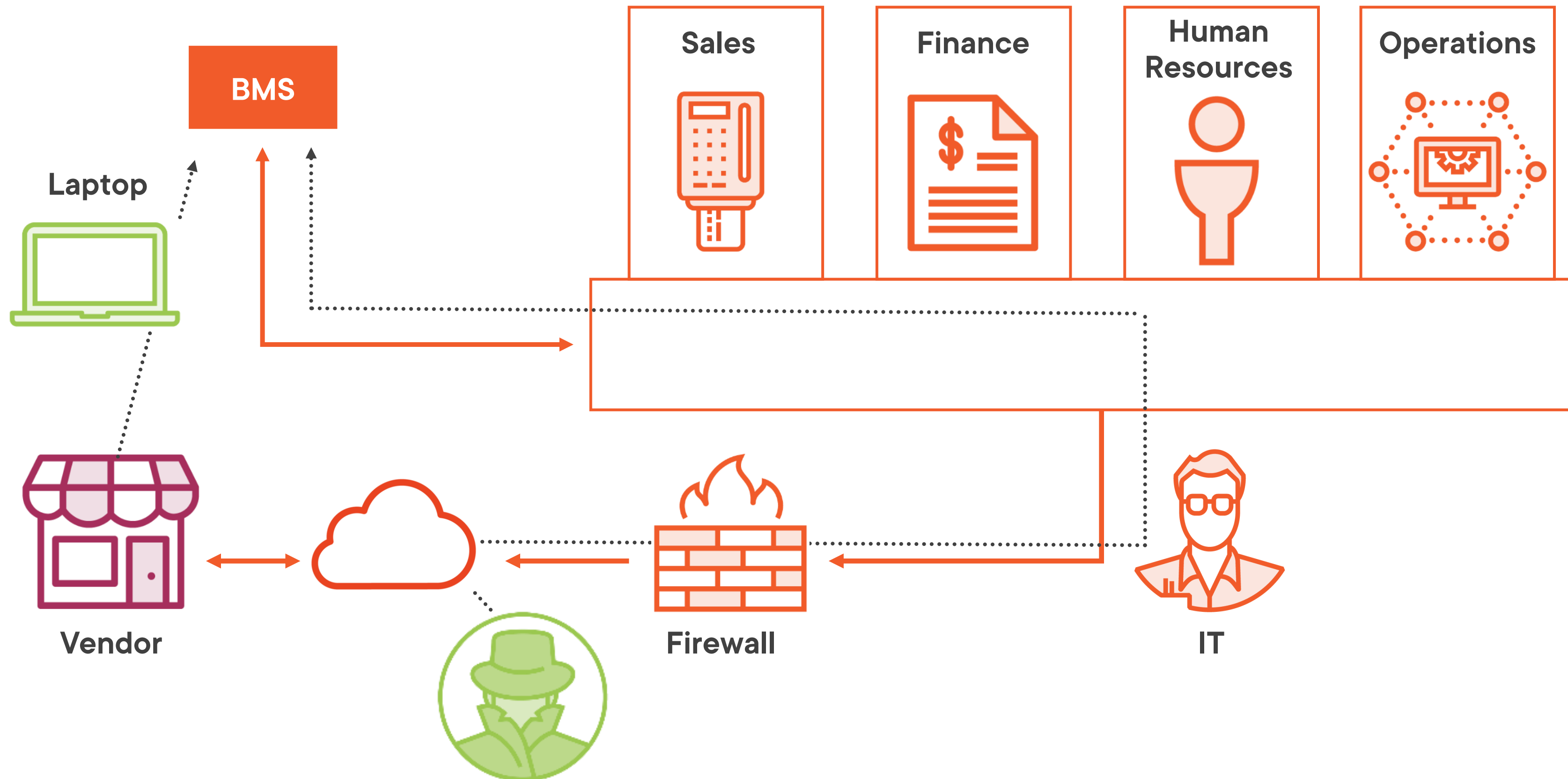
# The Way It Happened



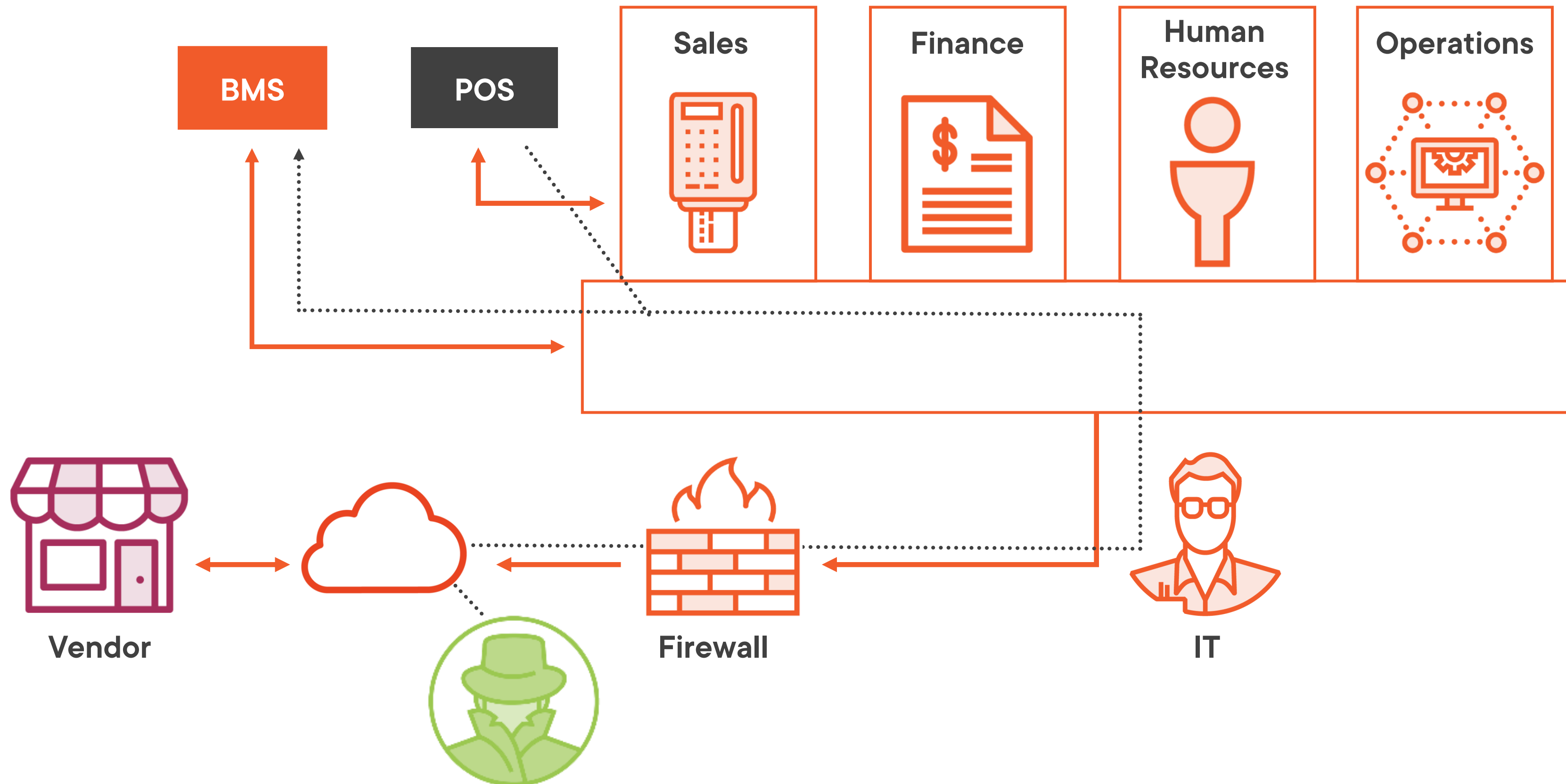
# The Way It Happened



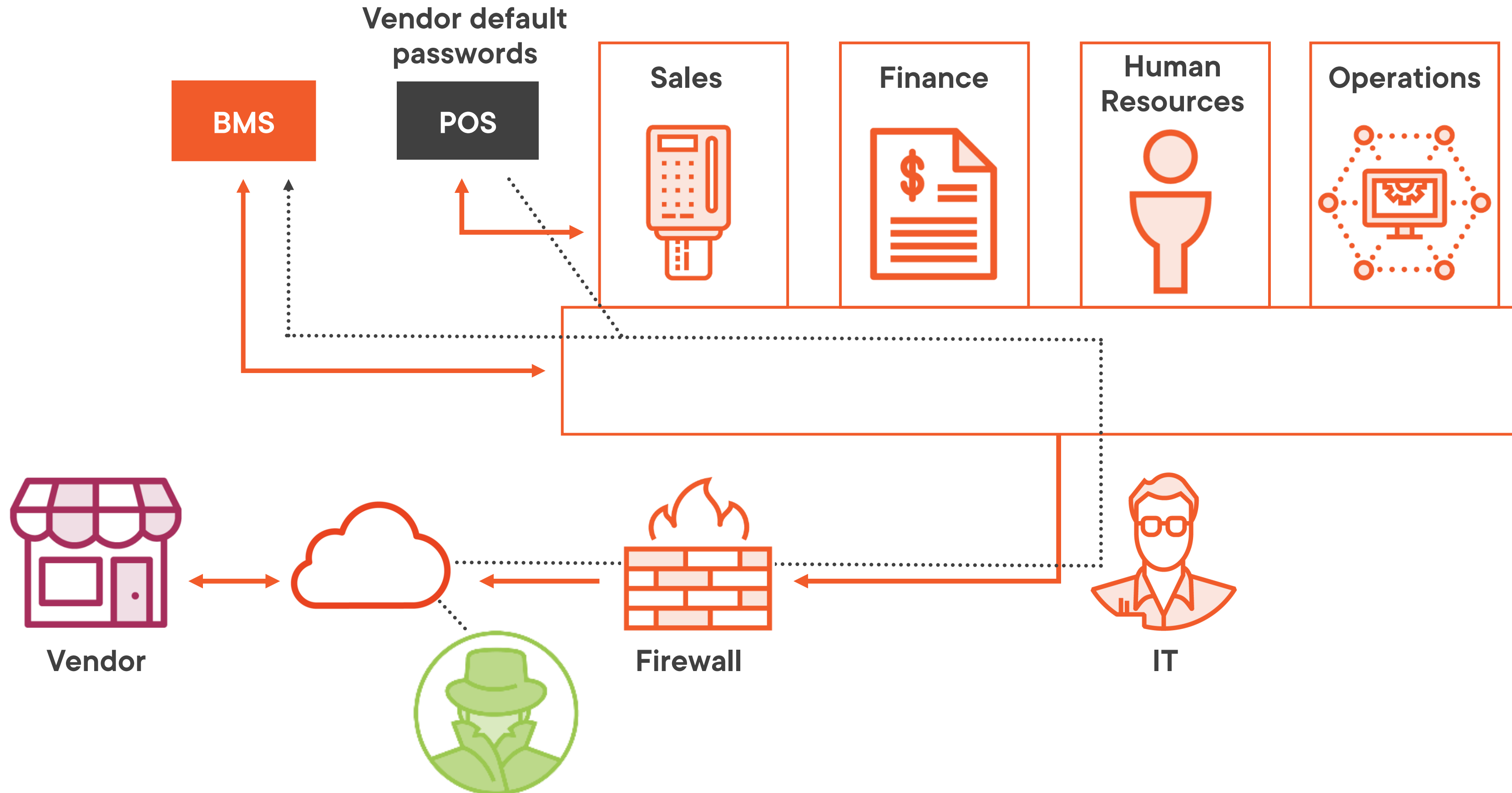
# The Way It Happened



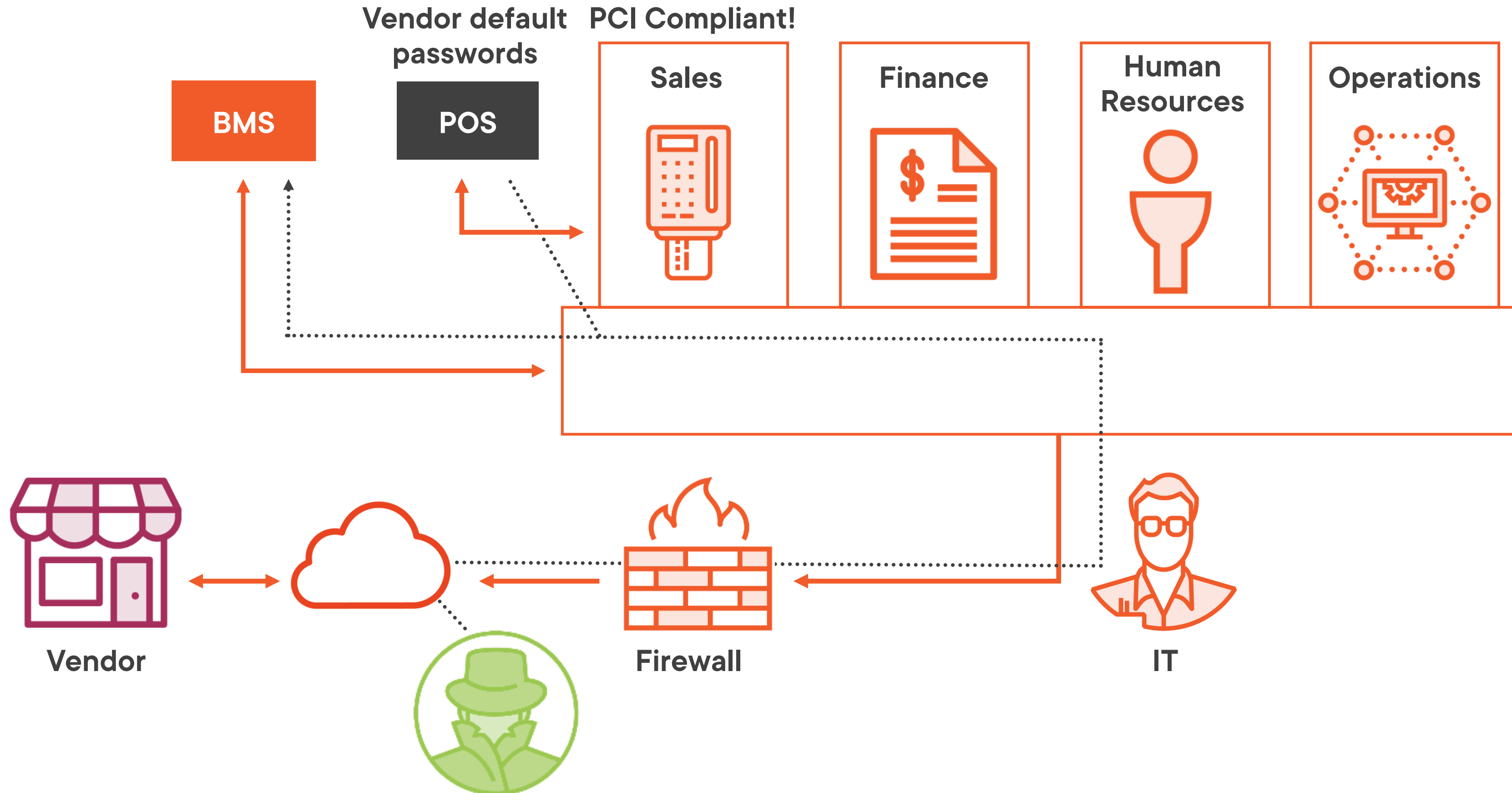
# The Way It Happened



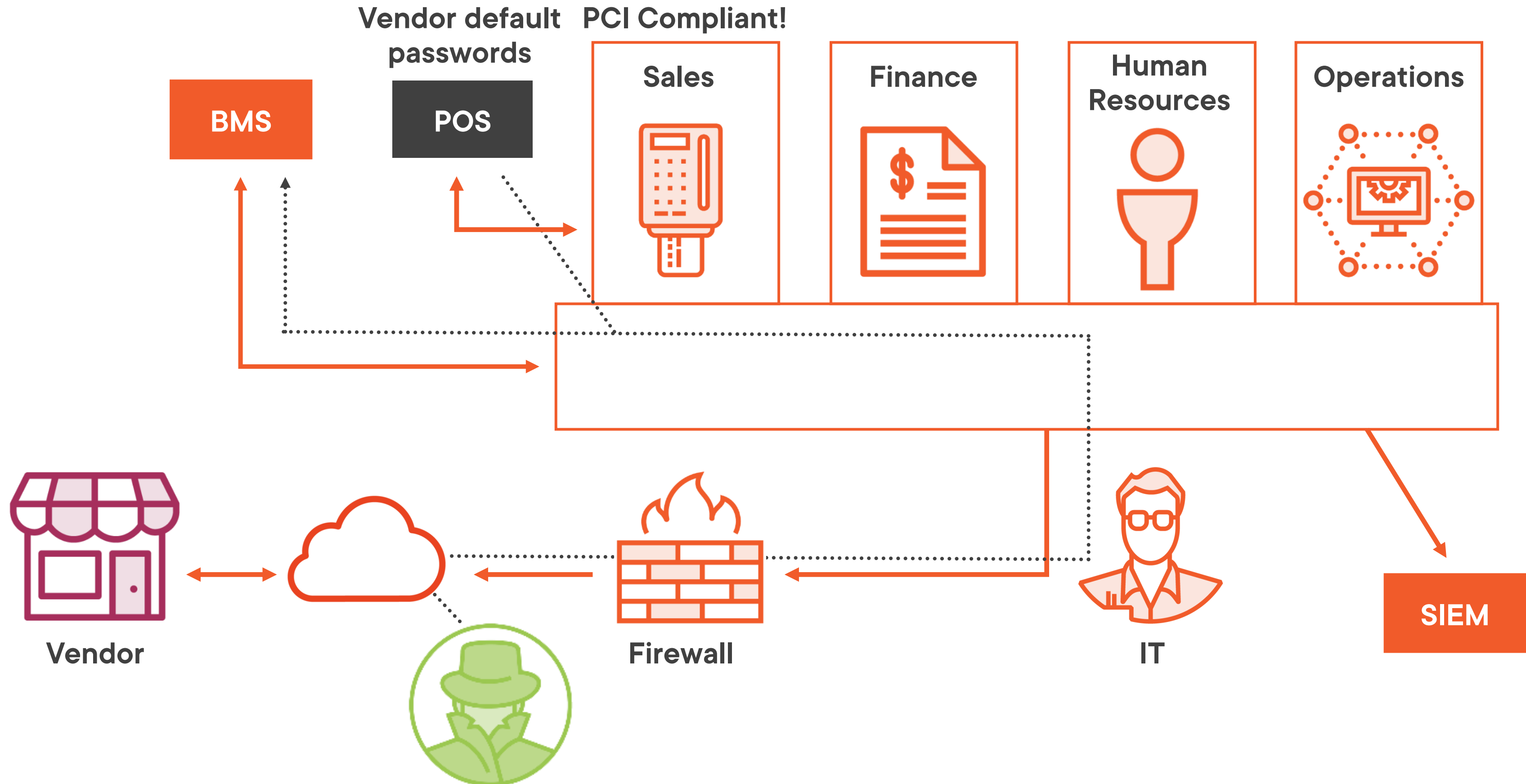
# The Way It Happened



# The Way It Happened



# The Way It Happened



## Key Points Review

**There were many mistakes that led to this breach**

- **Therefore there are a lot of lessons for us to learn**

**Network security is essential to secure and reliable business operations**

