CYBERSECURITY & ACCOUNTING

MOSES VARGHESE
LUMOS TECHNOLOGY SERVICES

LUMOSTS.COM

Of Vital Importance

As technology continues to advance, the need for robust cybersecurity measures in the accounting industry has become increasingly important. In this presentation, we will explore the intersection of cybersecurity and accounting, understand the threats professionals face in the field, and discuss best practices for ensuring the security of financial data.

01

Intersection of Cybersecurity and Accounting

A PARTNERSHIP

Critical Data

Smaller organizations are often targeted by cybercriminals due to a lack of data security measures making them vulnerable to attacks. Accounting firms, especially small to medium-sized, are attractive targets for hackers because they handle personal information, business information, and client financial data.

CLIENT PERSONAL INFORMATION

BUSINESS INFORMATION WITH PERSONAL DATA

FINANCIAL INFORMATION

Legal Implications

VIOLATION OF PROFESSIONAL RESPONSIBILITY

CLIENT IDENTITY THEFT SUIT

LEGAL FEES

Accounting firms are confronted with the challenge of potential data breaches, which not only harm their reputation but also violate client confidentiality.

Impact of Cyber Attacks

DATA LOSS & THEFT

FINANCIAL LOSS

REPUTATION

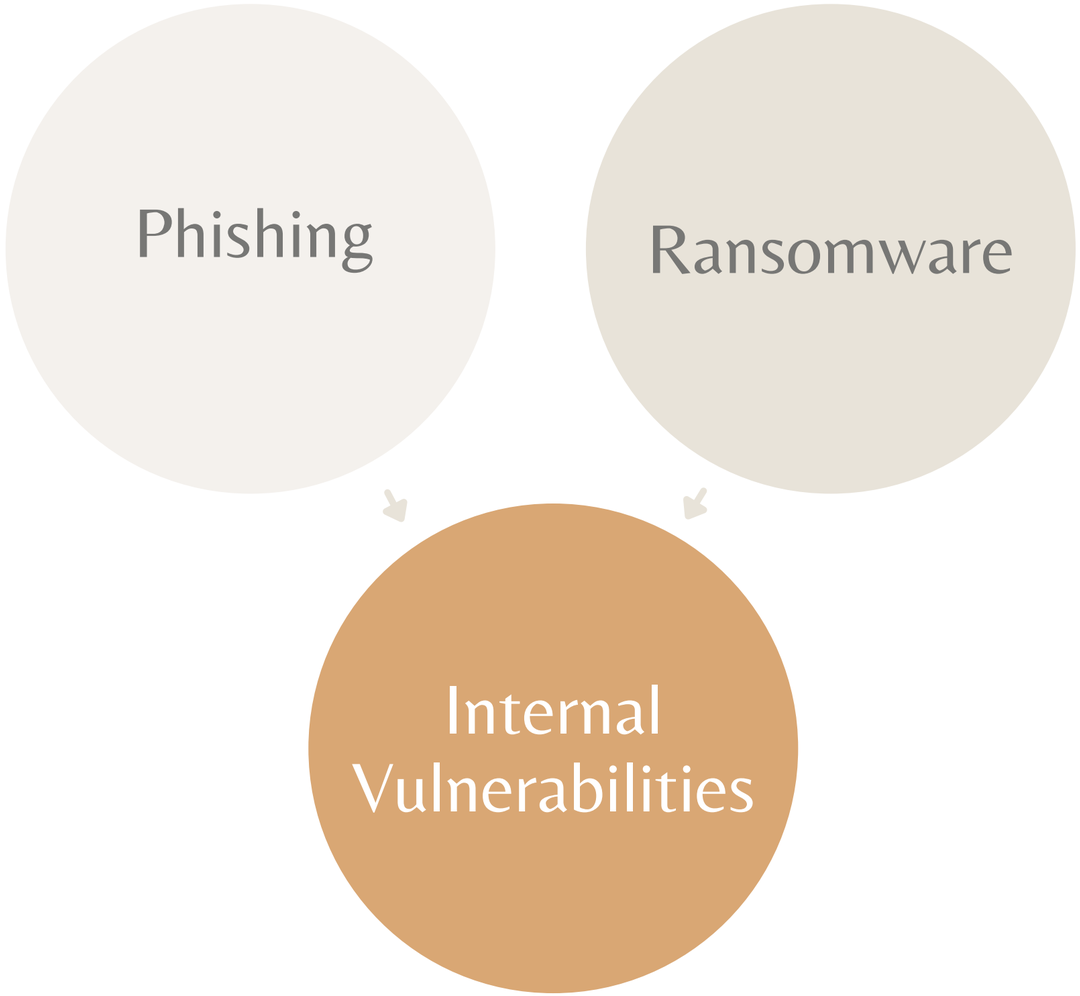
Consequences of cyberattacks vary in potency depending on the size of the breach.

02

Cybersecurity Threats In Accounting

THEY'RE OUT THERE

External threats paired with internal vulnerabilities makes an easy target.



Phishing

Deceptive emails requesting sensitive information to gain access.

- Rule creation
- Search for high-value or easy targets
- Modify and send emails using your account

Ransomware

Malware that encrypts files for ransom.

- Perimeter defenses are breached
- Bad actor has access to network and devices
- Covertly spread malware to critical systems
- Encrypt files
- Notify organization demanding ransom

Internal Vulnerabilities

Authorized company users.

- An untrained employee clicks on a link in a phishing email
- Negligent contractor or vendor who compromises security by misusing assets
- User access to network segments outside of scope for a particular role
- Lack of oversight of users with administrative privileges

Notable Attacks

2013

Adobe

- Malware
- 38M PII stolen
- Conversion to SaaS
- Poor IT security practices

2023

Progress Software

- Zero day threat
- 94M users impacted
- MOVEit software
- $15M+ damages

2023

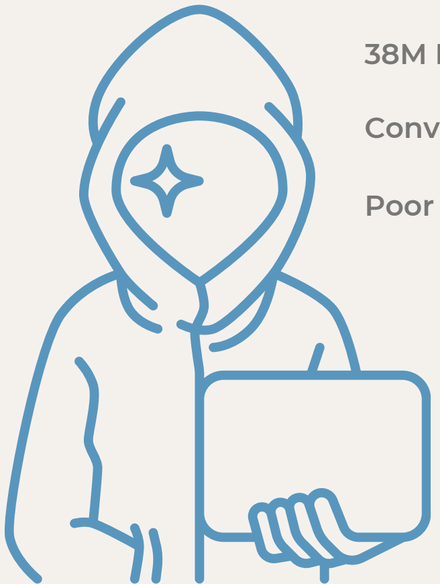
AT&T

- Undisclosed breach
- 70M+ customers
- Undetected for 2 years
- Multiple lawsuits

2024

Prudential

- Ransomware
- 16.6M PII leaked
- Failed negotiations
- $300M+ ransom payments



03

Best Practices to Prevent Vulnerabilities

ARM YOUR ORGANIZATION

Backup & Disaster Recovery

Procedures and policies that ensure quick recovery of data in case of a disaster.

01. Immutable data backup

02. Test restore functionality

03. Create system & server golden images

04. Cyber Incident Response Plan

Email Security

01

End-user training

02

STARTTLS encryption

03

DKIM and DMARC enabled

04

SOC monitored email security

End-user Training

Establish email use policy

Expectations regarding how email is utilized.

Annual training

Create a security-focused mindset.

Simulated phishing attacks

Ensure retention and compliance.

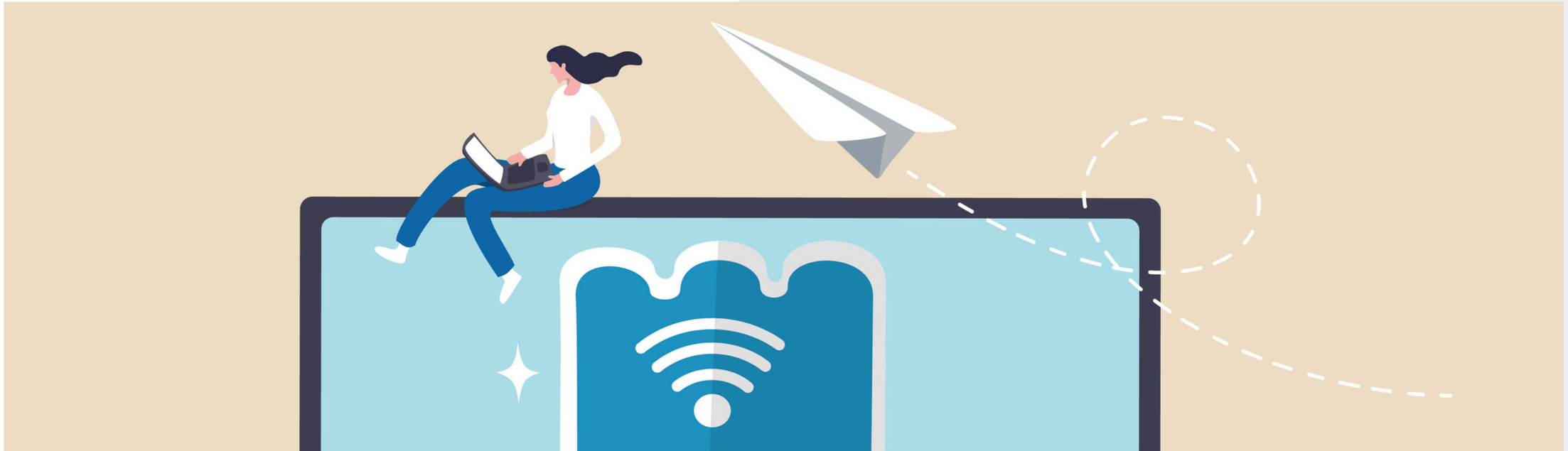
Secure Access to Network

Remote Desktop Protocol

- Only allow access with use of a VPN
- Lockout policies
- Multi-Factor Authentication
- Block multiple failed login attempts

Password Policies

- Strong passwords
- Utilize a password manager
- Change annually
- Screen passwords against known password lists



Firewalls

Early detection to prevent unauthorized network entry

- Configure firewall using best practices
- Monitor and maintain firewall rules
- VPNs to connect to vendors, remote users, and clients
- Continuous SOC monitoring

Network Segmentation

- Security layer
- Restrict access to main network
- Secure critical data and control access
- Segment IoT devices from main network

Vulnerability Scanning & Penetration Testing

- Quarterly vulnerability scan
- Penetration test annually
- Required by most compliance frameworks
- Reduce liability & risk

Monitored EDR & MDR

- Live monitoring of network traffic and devices
- Mitigate intrusions before they spread
- Proactive approach to security
- Reduce liability & risk

Questions?

LUMOS

Technology Services

THE CYBERSECURITY EXPERTS

EMAIL
moses@lumosts.com

PHONE
214-210-1121

WEBSITE
lumosts.com