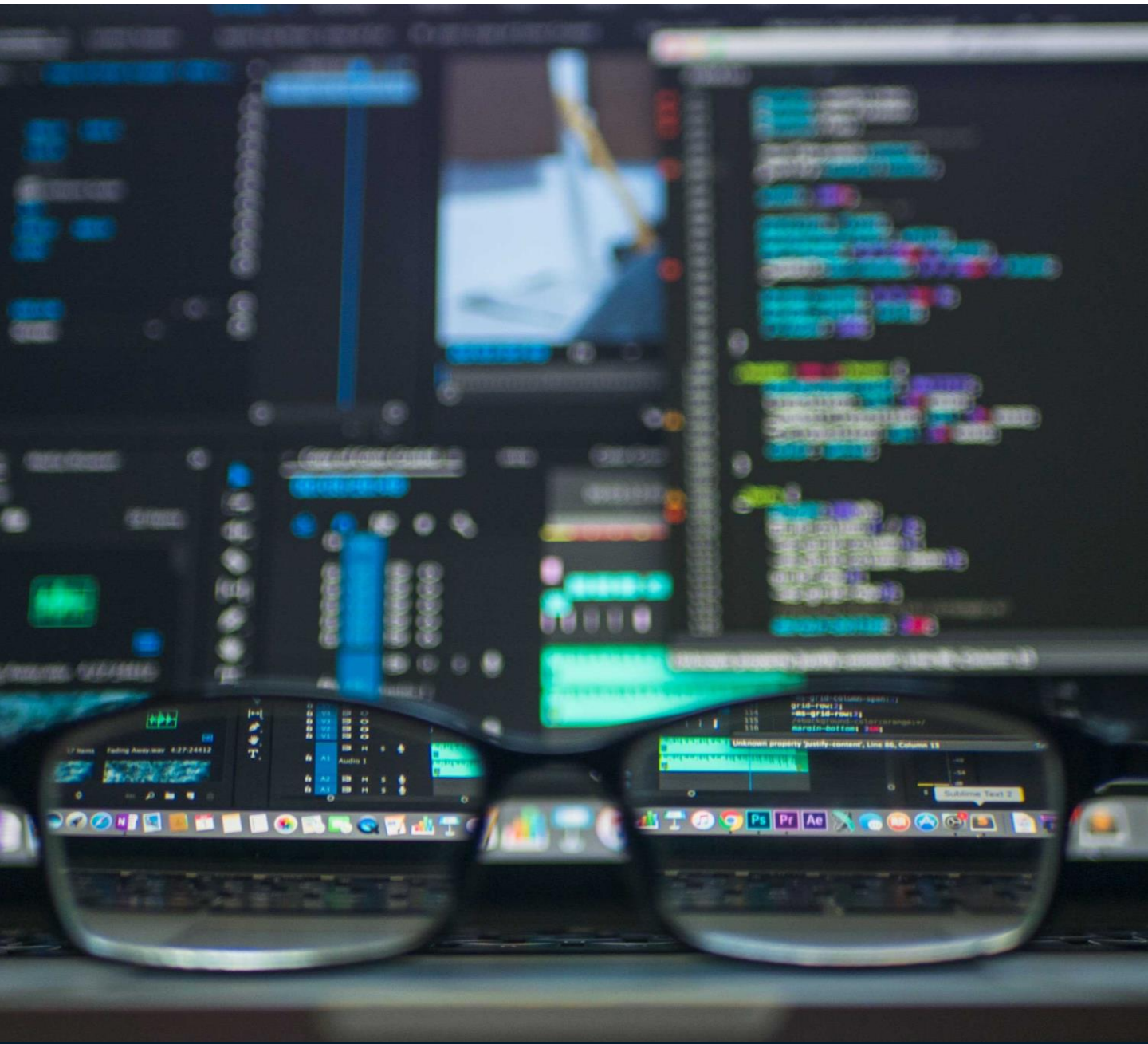
Finstein

Covid19 – Cyber Security Considerations for Work from Home



Covid19 – Cyber Security Considerations for Work from Home

Due to lockdowns imposed by various governments, organizations were forced to change their business models and the way employees worked.

Many organizations implement work from home policies and practices. They were forced to embrace latest technologies to enable employees to work remotely away from the office network.

There is a large scale increase in the cyber attacks after the onset of Covid-19. Cyber criminals are trying to take advantage of weary public sentiment on the pandemic situation.

Practices adopted by organizations to implement remote working.

Moving in-house hosted applications to the cloud

Subscribing to a cloud firewall

Using VPN to connect the Organization network

Subscribing to video conferencing tools

Improving Data Loss Prevention practices

Finstein

Covid19 – Cyber Security Considerations for Work from Home

Cyber security practices to be considered while working from home. While implementing suitable controls, ensure to review existing policies and procedures

Managing Access to Assets

- Enforce multi-factor authentication
- Ensure remote services and profiles are active only when required
- Continuously assess capacity and load balancers to ensure optimal system performance/response.
- Monitor access and logs for critical servers, applications and databases

Managing Network and Connectivity Security

- Employ IP Address restrictions to direct traffic to specific systems as appropriate
- Implement network filtering mechanisms
- Consider implementing Layered security and review controls around VPN
- Review any third parties connecting to the Organization's network

Vulnerability Assessment and Penetration Testing

- Perform Vulnerability Assessment and penetration testing for critical information assets
- Consider conducting a Red Team assessment

Managing End Point Security

- Ensure that Operating System and applications on endpoints are upto date.
- Implement network filtering on endpoint devices
- Ensure virus and malware protection are enabled and upto date
- Consider implementing a comprehensive Data Loss Prevention (DLP) solution
- Ensure Organization data is not stored on personal computing devices

Maintain Business Resilience

- Ensure to have a Disaster Recovery site
- Ensure data at end points are backed up periodically
- Ensure employees have adequate power backups to meet business SLA requirements

Employee awareness and training

- Conduct adequate Employee awareness and training to detect social engineering and phishing attacks

Key Takeaways

- Embrace digital solutions to ensure business objectives are achieved
- Assess cyber security risks while implementing work from home practices
- Review any Information Assets that are vulnerable after implementing work from home practices
- Implement suitable controls to ensure vulnerabilities are remediated

About Finstein

Finstien is the next generation consulting firm, we leverage heavily on innovative technologies and some amazing minds to provide insights and value addition to our clients. We are severely passionate to deliver outstanding quality

Visit us:

India
First Floor, New no 43 Old no, 65
South West Boag Road
T Nagar Chennai 600017

Singapore
No.3, Shenton Way, # 15-10,
Shenton House,
Singapore 068805

Reach us on: **www.Finstein.ai**

Our Services

- Accounting and Assurance
- Tax Advisory and Compliance
- Risk Advisory
- Cyber
- Data and Insights

Contact

Praveen Kumar

Partner: Risk, Cyber and Analytics

E: Praveen@Finstein.ai

M: +91 99400 16037