WEBINAR

How to Prevent Cyber Attacks that Can Destroy Your Business

April 22 at 10:00 AM

PRESENTED BY INFUZION SOLUTIONS | INFUZION.COM

Meet the Presenters

Jon McKinnon
IT Director

Toby Olson
Director of Sales and Operations

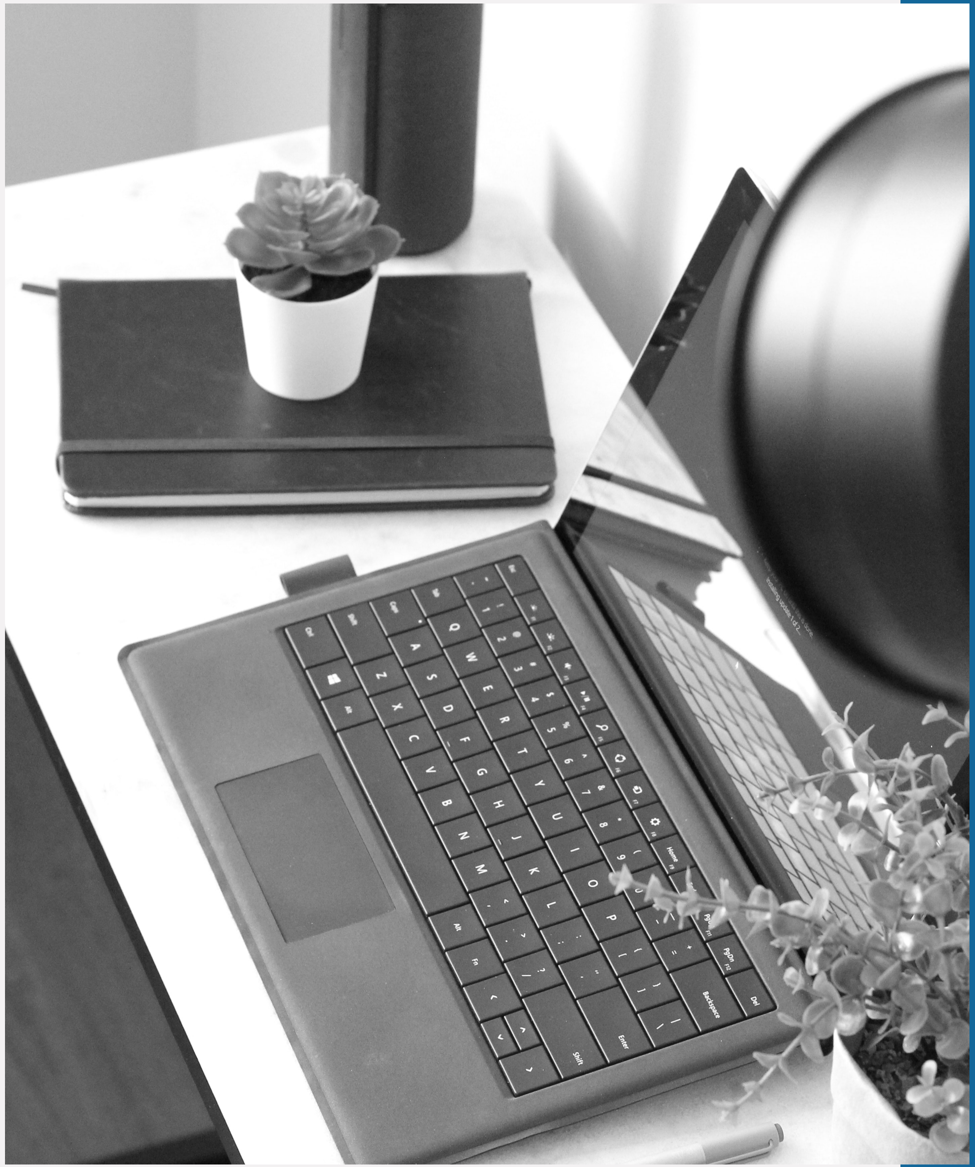
About Infuzion Solutions

Infuzion Solutions is a certified Microsoft partner and small business consultant located in Knoxville, TN.

Businesses use our software solutions and services across various industries, including wholesale, distribution, healthcare, higher education, and professional services.

Our solutions help maximize software investment while improving staff productivity and company profitability.

We not only assist small to mid-size companies in implementing new administration and accounting software but consult with those wishing to improve their business processes.



Companies that don’t stop data breaches have a 40% survival rate

Smallbizdaily.com

73% of social engineering attacks were coordinated against careless employees with little technical experience.

Murray Goldschmidt, COO of Sense of Security

Overview

- Account Security
  - Locking down accounts
  - Limiting access
  - Suspicious activity
- Securing Your Front Gate
  - Reinforcing firewall
  - Lockdown wireless & cloud

- Patch Management
- Backups & Disaster Recovery Plans
- Going the extra mile
- Review

Is my organization properly leveraging our current investments?

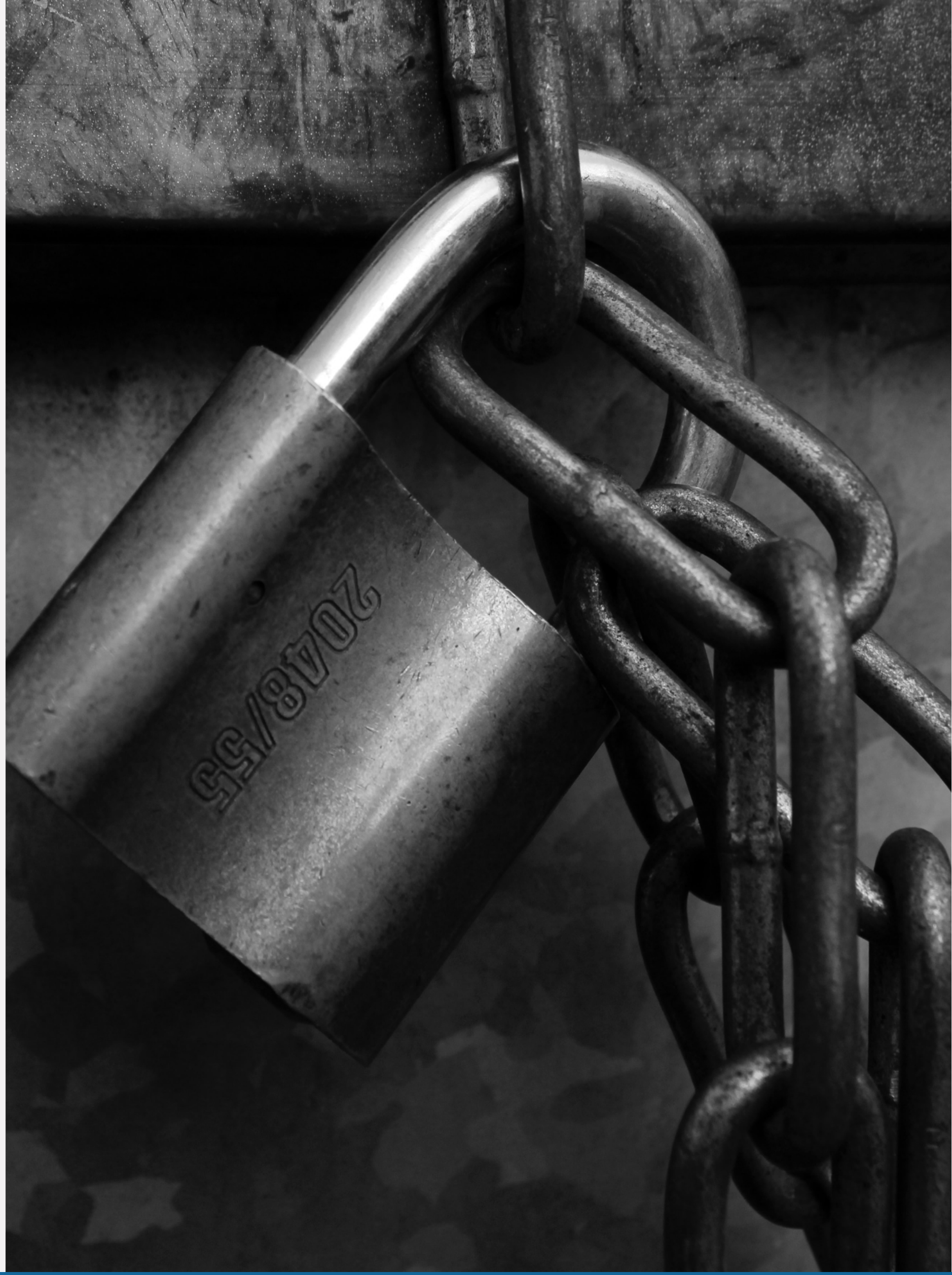
Have we tested those items and do they meet our expectations?

What do we need to do next to move toward a more secure organization?

Account Security

Lockdown Accounts

- Workstation admin accounts
- Server admin accounts
- Domain admin accounts
- Temporary domain admin accounts
- Admin passwords need 15 or more characters to stop stored hashing



Account Security

Limit Access

- Don’t remote to servers from end user computers
- Only allow remote access to DCs from trusted workstations
- Block / limit internet access on DCs
- Stop using Single sign-on (SSO)
- 12-character passwords, expiration, and history

- Use MFA (multi factor authentication) as much as possible
- Smart card-based authentication
- 3rd party MFA (MS has a list of providers)

Blocking an install or scanning a file is not enough!

Suspicious Activity

☑ Start with a traditional antivirus system (Bitdefender)

☑ Add a second layer of client protection for newer threats (Redcloke, EDR)

☑ Add Patch Management to your systems (Bitdefender)

☑ SIEM (Security Information and Event Management)

☑ Uninstalled / don’t install unused software

Start with a traditional antivirus system

- Real-time scanning based on signatures and behavior
- Scheduled deep systems scans
- Software firewall and web filtering
- USB device access policy / lockdown

Add a second layer of client protection for newer threats (Redcloak, EDR)

- Scan memory for attacks that no longer store files or run installs directly
- Remotely isolate affected devices on the network
- Block suspicious scripts on all servers and endpoints

SIEM (Security Information and Event Management)

- Collect, review, and get alerts on threats from all endpoint in one place
- Monitor the system internally and/or have it monitored
- Infuzion Solutions can do solo or joint system review daily or weekly
- A third-party security company can do 24/7 real time monitoring

Uninstalled / don't install unused software

- The more software installed on any server or workstation, the higher the risk

- If it is not mission critical, do not install it

- If it was a one-time use tool, uninstall it

- Remove java wherever possible

- Update software, removing outdated versions

Secure the Front Gate

- Reinforce your firewall (more than just updates)
- Lock down your wireless (could include wired)
- Lock down cloud resources such as Office 365 or remote access tools

Reinforce Your Firewall

- As always start with a current firewall, under support, and up to date
- Make sure Gateway AV filtering is enabled
  - Use real time cloud scanning if available
  - Customize setting (example: block file transfers with older VBA code)
-

  Enable and configure Intrusion Prevention (all zones)

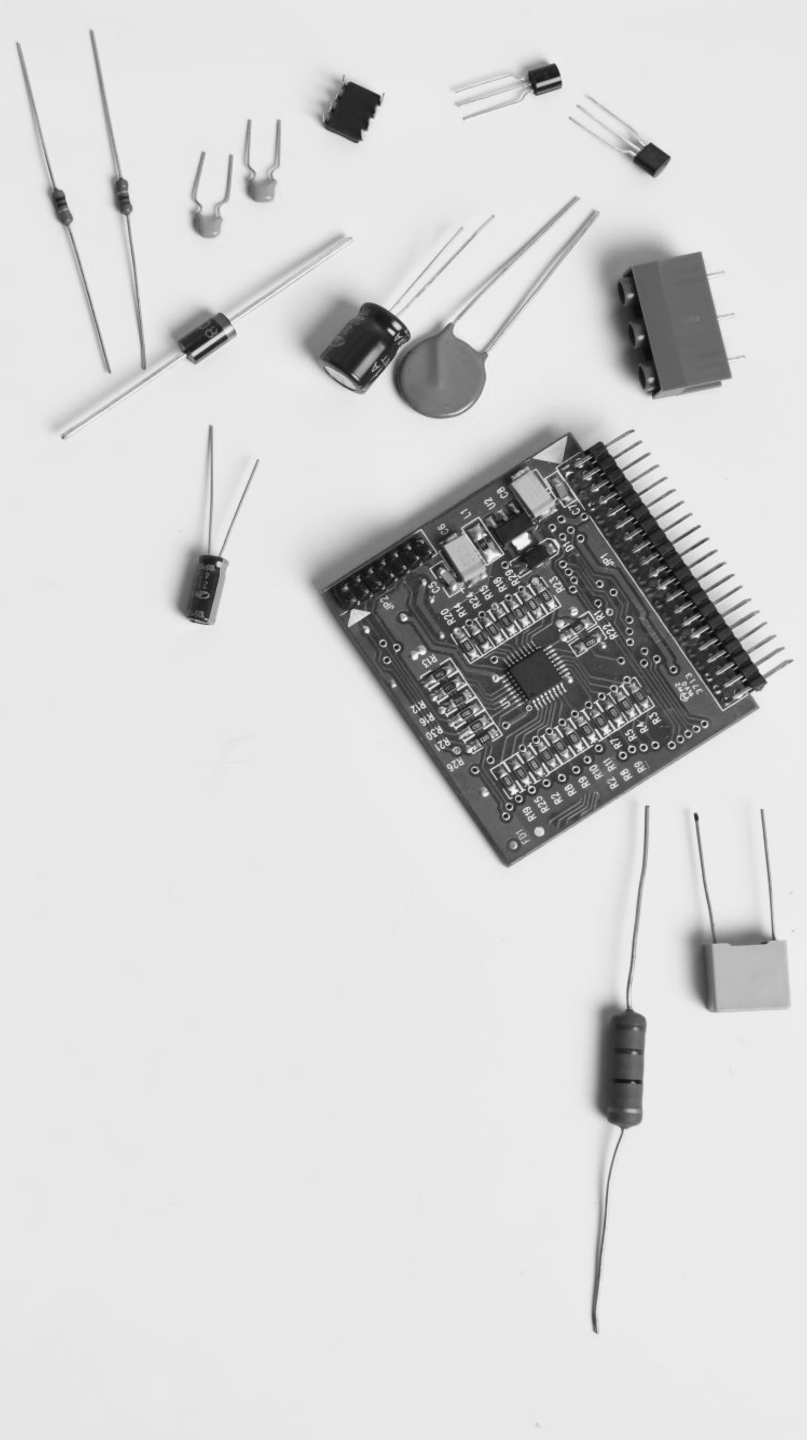
- Enable and configure Botnet Filtering (known bad actors)
- Enable and configure Content filtering
- Enable and configure App Control
  - Customize setting (example: block TOR and Encrypted Key Exchange)
- Enable and configure Deep Packet Inspection

Lock Down Your Wireless

- Make sure you have a secure and segregated guest network
- Devices that just need internet access should be on the guest network
- Limit access from wireless devices to only necessary resources
- Whitelist access only for corporate network

Lock Down Cloud Resources

- Use Office protect offered by Infuzion Solutions to enforce a security template on your O365 environment
- Subscribe to Office protect monitoring and alerts ($1, per user, per month)
- Enable MFA (at least for accounts with admin access)



Patch Management

- Regularly scan for software vulnerabilities on servers and endpoints
- Get alerts and insight on what computers are most at risk
- Automatically install patches to mitigate those risks

The Last and Most Important

- Backups and Disaster Recovery (beyond the natural)
- A full DR test (more than a spot check)
- The Plan (have it all documented; reduce panic, knee jerk reactions, and recover faster)

There Are Three Types of Companies:

🔒 Those that will be hacked.

🔒 Those that have been hacked.

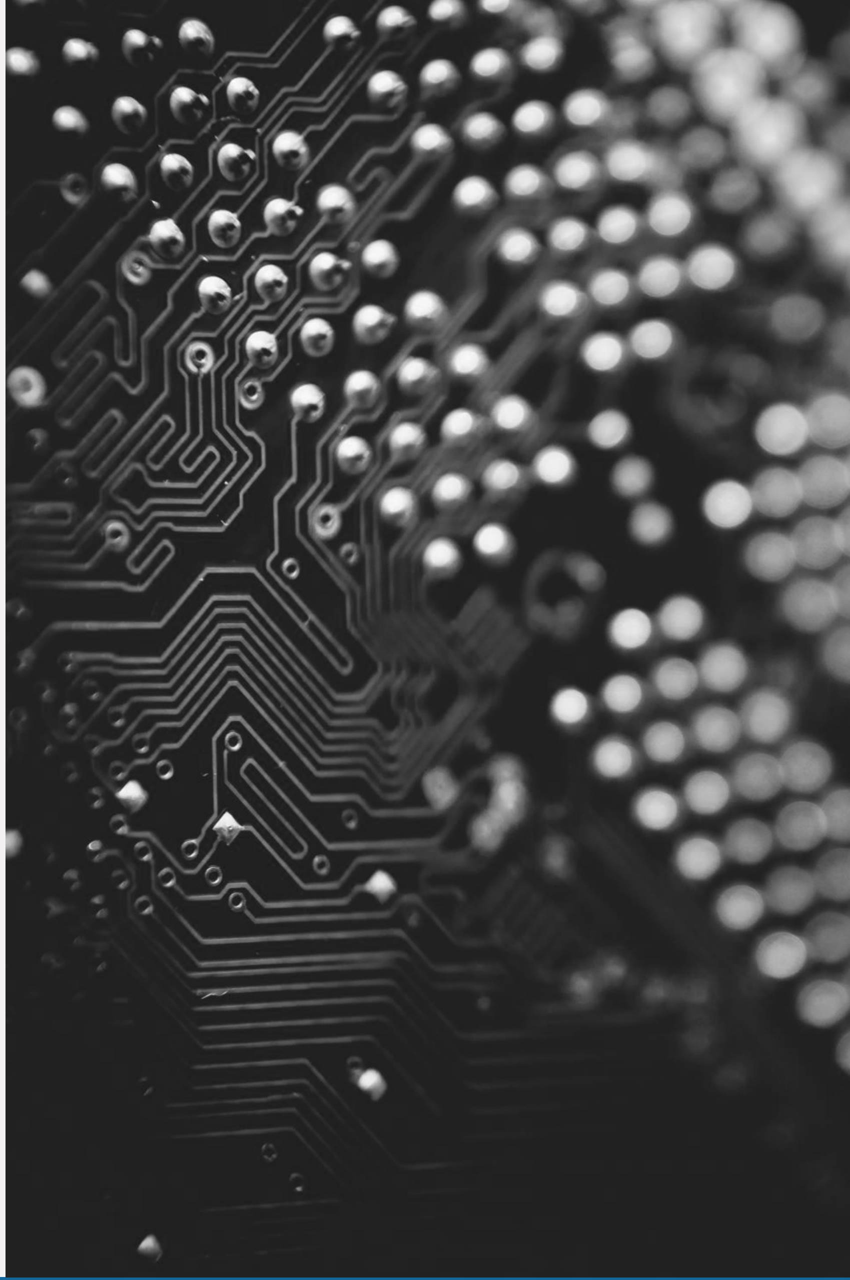
🔒 Those that will be hacked again.

Backups and Disaster Recovery

- As always you need backups, the more frequent the better
- Replication is great for business continuity, but a compromised replica server is no better than a compromised production server
- The primary or secondary backup server needs to be off your domain
- If the secondary backup server is local keep it on a separate network
- No domain account should have access to the backup server or data.
- Even with a secondary backup server isolated onsite, you should have an offsite copy of your data (secondary backup server can be in the cloud)

A Full Disaster Recovery Test

- Do all you servers restore as expected?
- Is you DR network and remote access preconfigured (test each time)?
- How long does it take to restore your mission critical servers?
- How much longer to get other necessary servers restored?
- Have a hot and cold restore plan and realistic timetables
- Do each of your plans as tested meet your requirements / expectations?



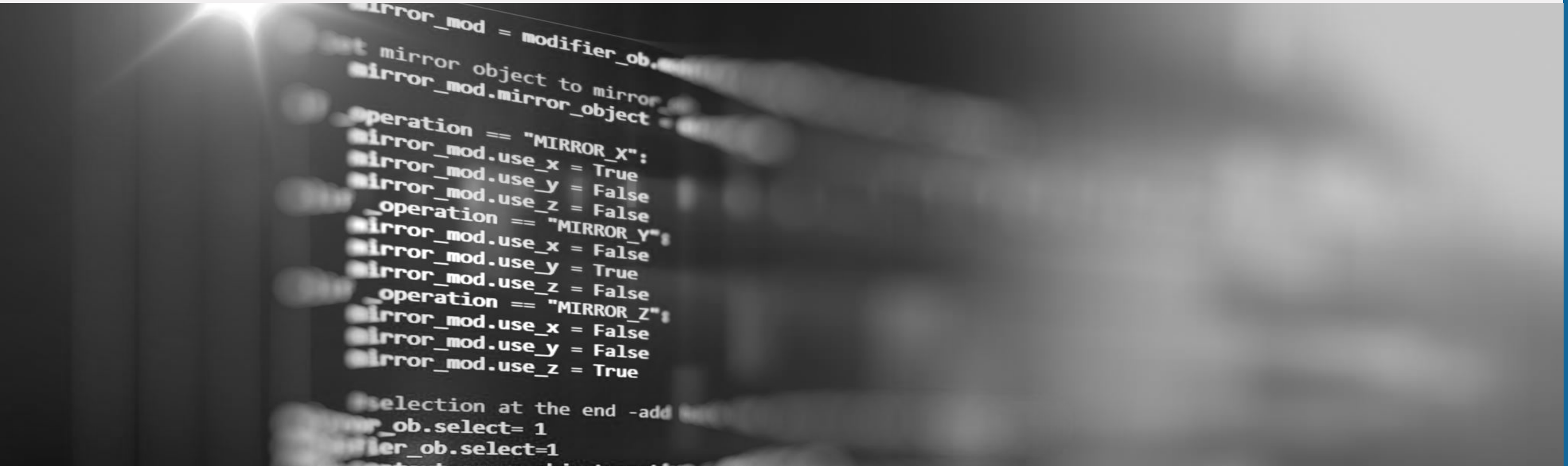
The Plan

Have it all documented. Reduce panic, knee-jerk reactions, and recover faster.

- DR (Disaster Recovery plan)
- BC (Business Continuity plan)
- IR (Incident Reponses plan)

Go the Extra Mile

1. Risk management plan (Internal) or solution (3rd party)
2. Vulnerability scans and remediation
3. Golden Images (standardized and secure images)
4. Data Encryption



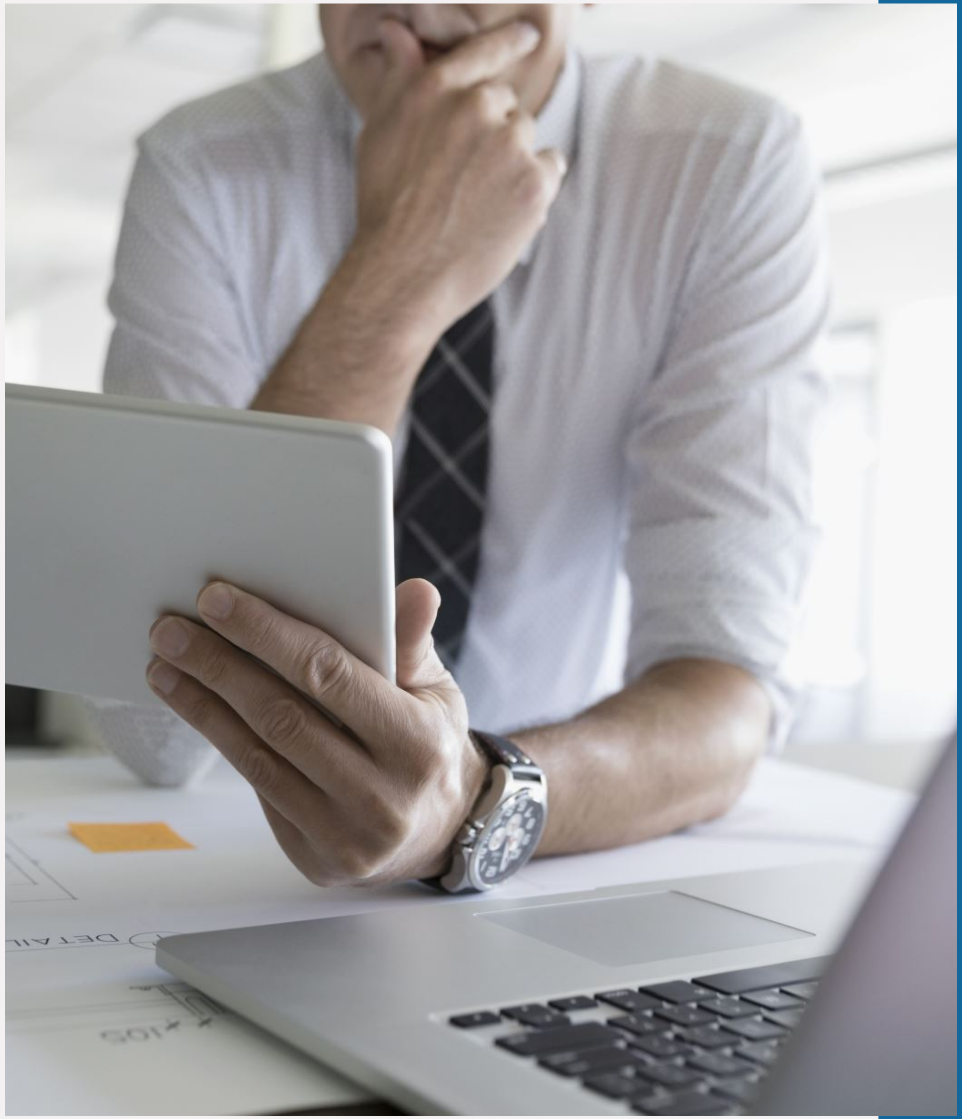
```
irror_mod = modifier_ob.
 mirror object to mirror
mirror_mod.mirror_object
operation == "MIRROR_X":
mirror_mod.use_x = True
mirror_mod.use_y = False
mirror_mod.use_z = False
 _operation == "MIRROR_Y":
mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
 _operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True

selection at the end -add
r_ob.select= 1
ier_ob.select=1
```

What can you live with or without? How much is too much?

Risk Management Plan (Internal) or Solution (3rd Party)

- Evaluate where you are weak
- Prioritize your efforts
- Identify weaknesses unique to your business, or of a higher likelihood than others



Vulnerability Scans & Remediation

- Based on your risk management plan, test expected weaknesses
- Evaluate and prioritize remediation base on weaknesses found/confirmed

Golden Images (standardized and secure images)

- Less human error when hardening new servers or workstations
- Reduce recovery or deployment time

Data Encryption

- Email - protect sensitive data being sent
- Protect data on your network, including VMs
- Protect endpoints, especially laptops

Review

- Pass the Hash/Suspicious Activity
- Securing the Front Gate
- The Last Line of Defense/Do the Extra

Infuzion Solutions is here to help. For more information, please do not hesitate to reach out.

Infuzion.com | info@infuzion.com

Q&A

Infuzion Solutions is here to help. For more information, please do not hesitate to reach out.

Infuzion.com | info@infuzion.com