The Top 10 things you must do to protect security systems from cyber attacks

Dave Tyson CPP, CISSP, MBA

Dave's Bio

- 16 Years in Physical Security Industry
  - Executive Protection
  - Investigations
  - Security Officers
  - Security Systems
  - Chief Security Officer
- 20 Years in Cyber Security Industry
  - Chief Information Security Officer
  - Cyber Security Consultant
  - Vulnerability Testing Company Owner
- Industry Experience & Credentials
  - Certified Protection Professional
  - Certified Information Systems Security Professional
  - MBA, Digital Technology Mgt.
  - 2015 President ASIS International

CISO INSIGHTS

Agenda

- Level Setting
- How Cyber attacks are carried out
- Top 10 Must do activities

CISO INSIGHTS

Why?

- 1 in 101 emails in malicious
- 32 % of email is actually clean enough for delivery

Malware Attacks Yield 1,425% Return on Investment

How cyber attacks became more profitable than the drug trade

How?

- **It was insecure to start with**
- **It was installed poorly**
- **It wasn’t maintained of monitored correctly**

What

- **Interconnectivity**
- **Complexity**
- **It's a weakest link discipline**

How Targeted Attacks Work

1

INCURSION

Attacker breaks into the network by delivering targeting malware to vulnerable systems and employees

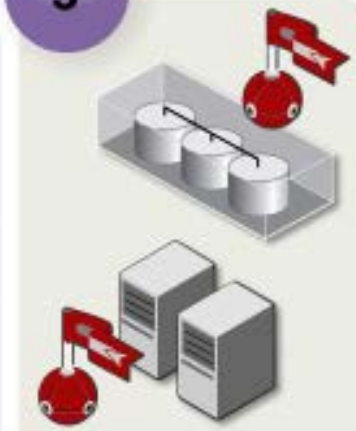
2

DISCOVERY

Hacker then maps organization's defenses from the inside

Creates a battle plan

3



CAPTURE

Accesses data on unprotected systems

Installs malware to secretly acquire crucial data

4

EXFILTRATION

Confidential data sent to back to enemy's "home base" for exploitation and fraud

Top 10 List

1. Do you have requirements for securing the tool or system?
2. Did it start secure?
3. Was it installed with a secure design?
4. Have the integration points being considered?
5. Is it tested for security before going live?
6. Are all the basics covered?
7. How will you know if the system is violated?
8. Who is going to monitor the system or tool for variance?
9. How will it be maintained?
10. Use security intelligence to understand your adversary's approach

CISO INSIGHTS

#1 - Do you have requirements for securing the tool or system?

- Security requirements must be developed if you want to let the technical team know your expectations!

CISO INSIGHTS

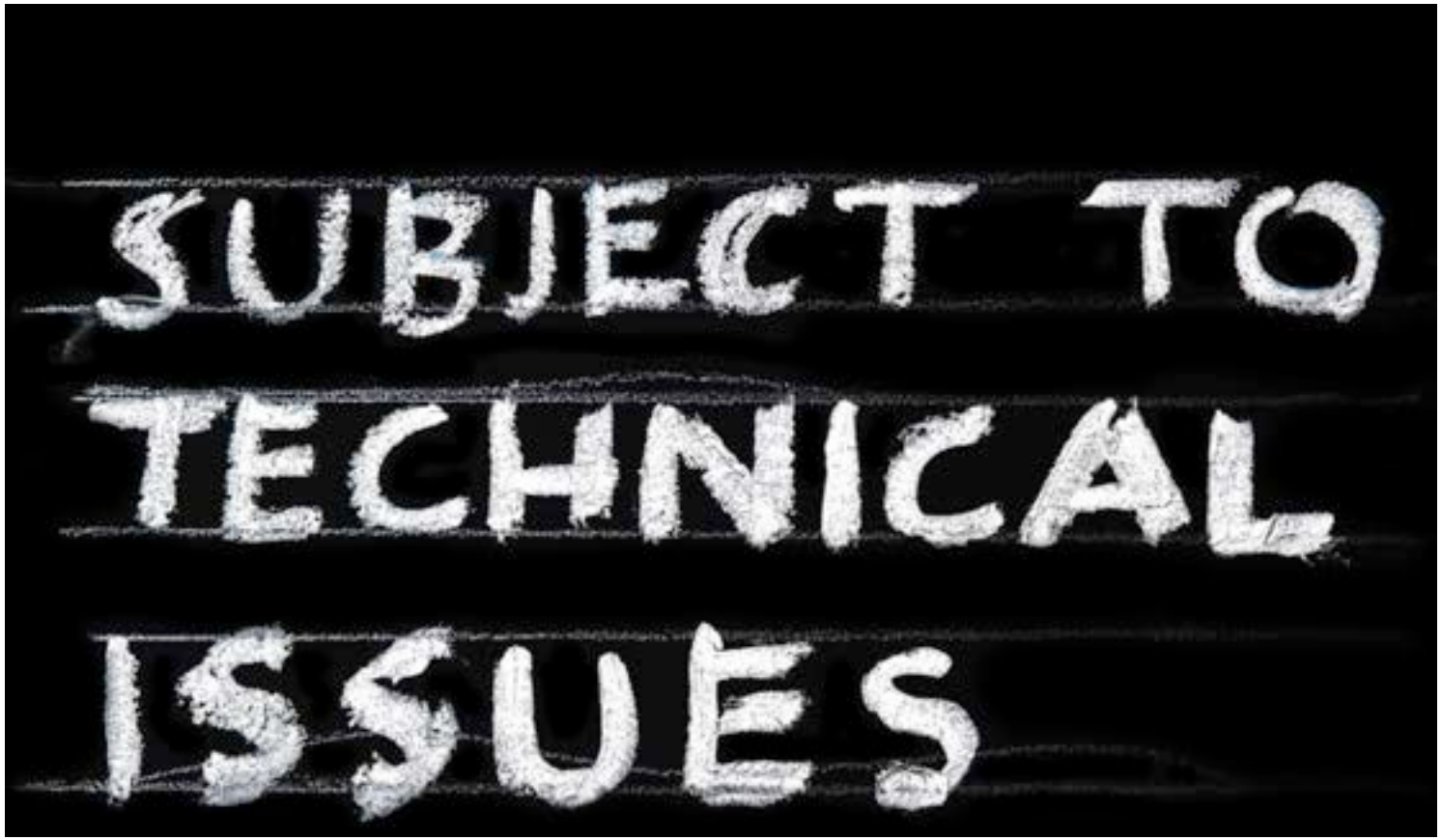
#2 - Did it start secure?

- Beyond the Vendor statements!
- What assurance level do you require?

#3 - Was it installed with a secure design?

- Was the a documented design created by an expert?
- Did the security requirements make it into the design?
- Was it installed according to the design?

CISO INSIGHTS



#4 - Have the integration points being considered?

- For systems that will be integrated or talked to, have the security issues been considered?

#5 - Is it tested for security before going live?

- Measure 6 times, cut once!
- No scope restrictions!
- Testing criteria should be added into requirements document!

CISO INSIGHTS

#6 - Are all the basics covered?

- Do you know all who will have access? Even in an emergency!
- Are the lock outs complete?
- Is there documentation?
- Is training included?

CISO INSIGHTS

#7 - How will you know if the system is violated?

- What does an attack look like for this system?
- What is the baseline, what does normal look like?

CISO INSIGHTS

#8 - Who is going to monitor the system or tool for variance?

- Who will monitor?
- What are escalation paths?
- What about reporting?

CISO INSIGHTS

#9 - How will it be maintained?

- **Who will patch and update it?**
- **What about end of life and replacement?**
- **Security disposal?**

#10 - Use security intelligence to understand your adversary's approach

- **Know thy enemy!**

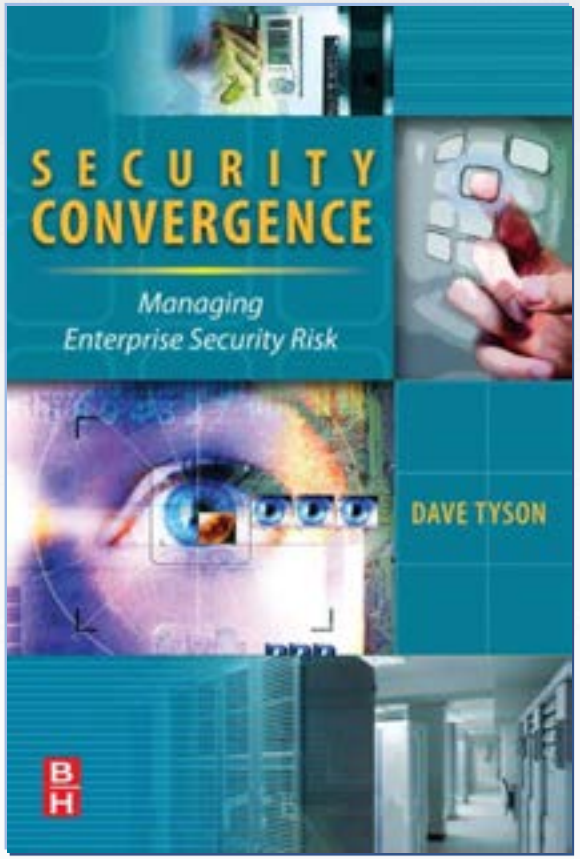
Summary

- Plan to succeed
- Work the top 10 list at a minimum
- Decide how much risk is acceptable
- Doorway to the data network

CISO INSIGHTS

Apollo Information Systems, Corp.

Dave Tyson
dave@cisoinsights.com



@cisoinsights

https://www.facebook.com/cisoinsights/

www.cybereasylearning.com

CISO INSIGHTS