WELCOME TO

Systems
Engineering &
Administration
Technology
User
Group

Wednesday, May 17, 2017

bringing IT together℠

Introduction to SEA-TUG

- Founded in 2001 by Rob Bergin and Steve Noel to help IT professionals in the seacoast collaborate and enhance their knowledge
- New steering committee formed July 2016
  - John Whelan, Pamela Capper, Deb Gale, PJ Soucy, Joel Wright, Derek Rolfe, Rob Maciorski, Terry Jamro, Chris Morris
- Part of larger user group communities
  - Boston User Groups, Meetup, etc.
- This is YOUR user group – help us make it better. What topics do you want covered? What resources can you contribute?

SEA-TUG

bringing IT together℠

Thank you to…

- Alexander Technology Group
  - Food/beverages
- Great Bay Community College
  - Meeting space

SEA-TUG

bringing IT together℠

Tonight's Presentation

Securing Your Organization
Where Do You Start?

George Magee

SEA-TUG

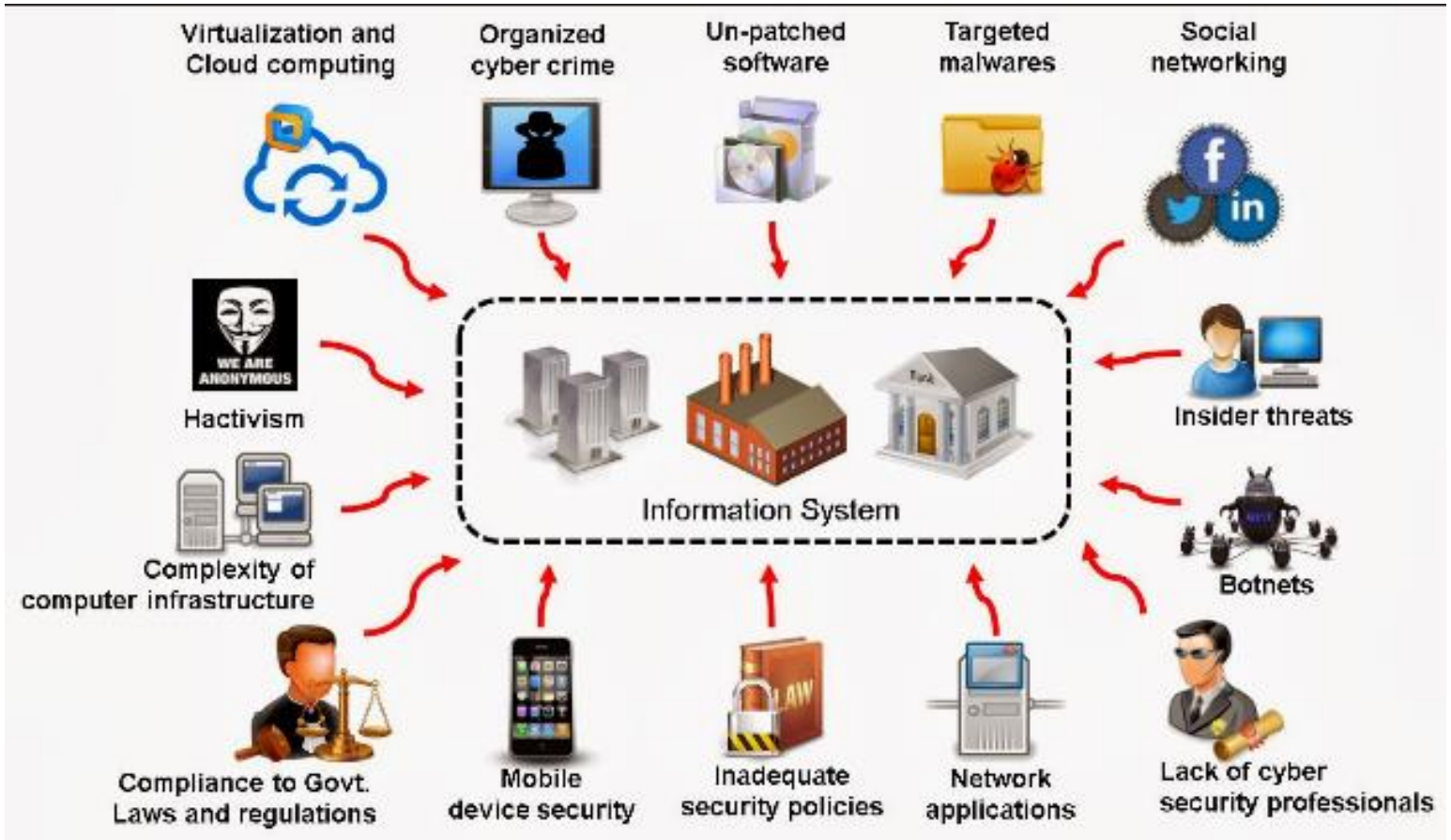
bringing IT together℠

Scenario

- You're given 3 months and $50,000 to improve your organization's security posture
- What to focus on?
- How to determine what's most important?
- Strategies to make multiple quick-hit wins given constraints

bringing IT together sm

Attack Vectors



SEA-TUG

bringing IT together℠

Protection Vectors

- Endpoint
  - Antivirus
  - Antimalware / Anti-exploit
  - Sandboxing
  - Whitelisting
  - Removal of admin rights
  - Firewall
- Gateway
  - Gateway AV
  - IDS/IPS
  - Geolocation
  - Default Deny (see C&C)
- GPOs
  - PW Policy and expiration
- Email
  - SPF / DMARC / DKIM
  - Reputation
  - Attachment blocking
  - Impersonation
  - New domains
  - URL Inspection
  - Attachment sandboxing
- Ad Blockers

Protection Vectors (Cont'd)

- Patching
  - No longer optional
  - Don't forget appliances
- Segmentation
  - Prevent spreading
- Proactive Inspection
  - FireEye / Onion
  - User education
- Flow data analysis
  - Long running connections
  - International connections
  - File transfers
- URL Filtering
  - Categories
  - Crowdsourced intelligence
- Centralized Logging
  - Used as a tool to identify infections and vulnerabilities
- Auditing
  - For forensics, and proactivity
- Administrative
  - H/W inventory
    - Rogue hardware reports
  - S/W inventory
    - Rogue software reports

Clever Command & Control

- Twitter
- DNS
- TOR

bringing IT together℠

Resources

- Top 20 Critical Security Controls

  https://www.cisecurity.org/controls

  https://www.sans.org/media/critical-security-controls/Poster_Fall_2014_CSCs_WEB.PDF

  https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

- Implementing an Effective Security Program

  https://www.sans.org/reading-room/whitepapers/bestprac/implementing-effective-security-program-80

- Configuration Baselines

  https://usgcb.nist.gov/usgcb/microsoft/download_win7.html

  http://www.nist.org/news.php?extend.204

  http://csrc.nist.gov/publications/PubsSPs.html

SEA-TUG

bringing IT together℠

SECURITY REPORTS

- Verizon Data Breach Investigation Report
  http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf
- AT&T Cybersecurity Insights Report
  https://www.business.att.com/cybersecurity/docs/vol5-datasecurity.pdf
  https://networkingexchangeblog.att.com/topics/security-in-the-enterprise
- Microsoft Security Intelligence Report
  https://www.microsoft.com/security/sir/default.aspx
- Symantec Internet Security Threat Report
  https://resource.elq.symantec.com/LP=3980
- Fortinet Threat Landscape Report
  https://www.fortinet.com/demand/gated/threat-landscape-report.html

bringing IT together sm

Top 20 Controls

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Access Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

bringing IT together℠

Quick Wins

- **DNS filtering with crowd sourced intelligence**
- **Employ automated malware detection tools to continuously monitor all nodes, log centrally**
- **Use remotely managed, centralized anti-malware infrastructure**
- **Turn off auto-run**
- **Automatically scan removable media**
- **E-mail content and web content filtering**
- **Enable anti-exploitation countermeasures (DEP, ASLR, EMET)**
- **Limit external devices to business need**