



Balancing Security & Risk Management

Randy Marchany

VA Tech IT Security Office & Lab

marchany@vt.edu



TEAMWORK

Share Victory. Share Defeat.



VA Tech IT Security Strategy

- Based on ISO 27002, NIST 800-53 Standards
- **Protect sensitive data regardless of location**
- Business process defines and trumps the security process if there is a conflict
- Don't care what comes in the net.
Worry about what leaves the net.

Things To Consider

- Learn the business process before applying security rules
- Data Owners must assess risk
- Compensating controls are good



Risk Based Security Management

- Application of rigorous and systematic analytical techniques to the evaluation of the risks that impact an org's IT assets and IT infrastructure
- Not a risk assessment



RBSM

Recommendations

- Start RBSM with a formal strategy
- Focus on risk as primary emphasis
- Ensure balance of preventive and detective controls



RBSM

Recommendations

- Establish and use metrics to measure success
- Collaborate between security and other business functions
- Continuously monitor to ensure RBSM protects the org over time

RBSM 10 Steps

- Develop basic security policies & standards
 - Must be enforceable
- Establish asset inventory
- Establish Info Sec Leads
 - Responsible for overseeing security in business areas

RBSM 10 Steps

- Create Enterprise Risk Committee
 - Senior mgt, ITSO, Legal, Audit, CFO, HR, Systems
- Define common approach to risk calculations
 - OCTAVE, Binary Risk Assessment, STAR, etc.

RBSM 10 Steps

- Establish threat & vulnerability mgt system
- Establish compliance to standards review process
 - Gap analysis against security policies, standards

RBSM 10 Steps

- Conduct basic risk assessments for 3rd party software/services
 - Vendor security questionnaires
 - Secure ok from data owners
 - Shared assessments

RBSM 10 Steps

- Build risk & Exception Tracking system
 - Track the state of risks in your environment
- Start Risk Assessment Awareness campaign
 - Shift from absolute security to risk focused culture

Types of Risk

- Strategic Risk
- Financial Risk
- Legal Risk
- Operational Risk
- Reputational Risk



More simply put...

“Determine what your risks are and then decide on a course of action to deal with those risks.”

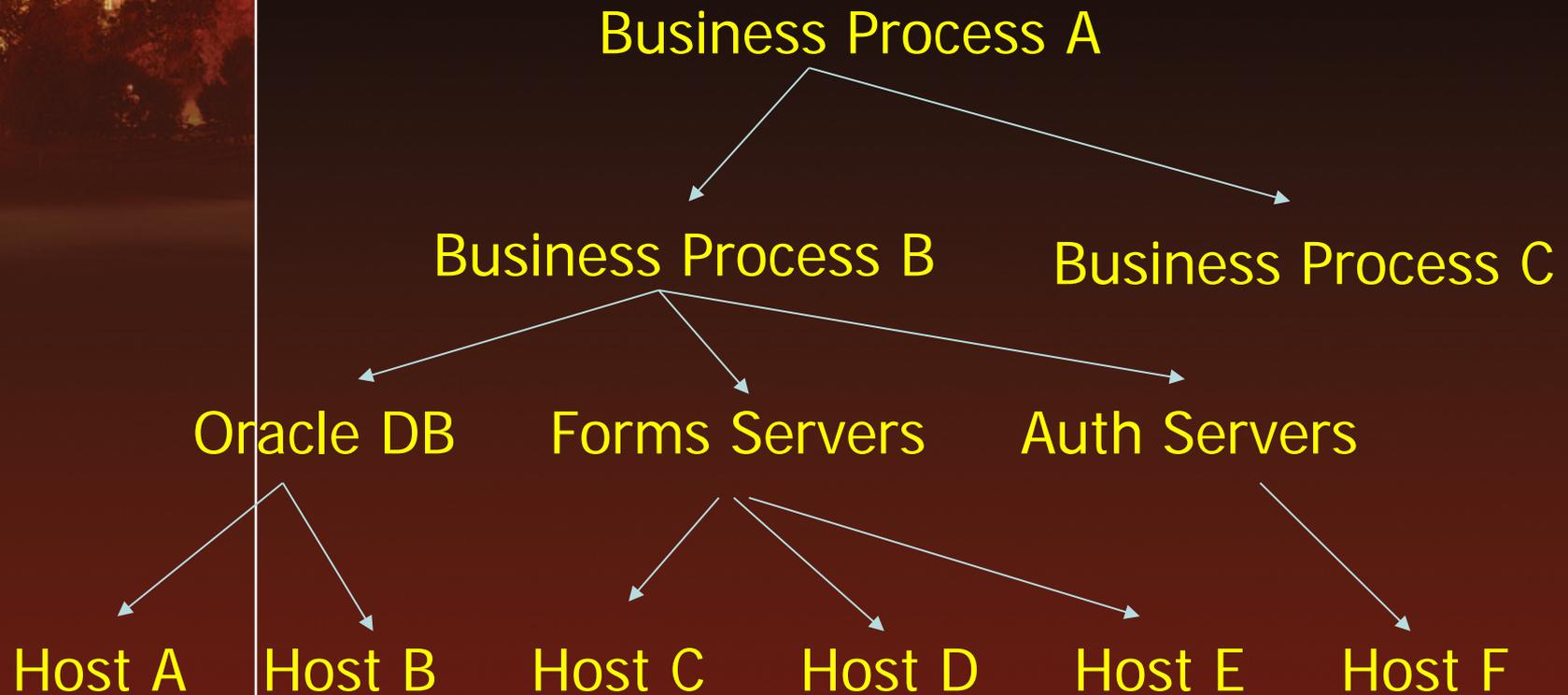
- Brian Davis (UVA)



Assets: More Than Machines

- Link Asset identification to the mgt org chart
- Assets can now be:
 - Sensitive Data
 - Physical systems
 - Groups of systems that support a service
 - Business process that requires a group of systems
 - Business process that depends on other business processes

Build Your DR





Kill Chain Attack

- Recon
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objectives

Minimizing Attack Surface

- Each control acts as a layered defense against the kill chain
- Some are preventive
 - Defend against inbound
- Some are detective
 - Defend against outbound

Change Defenses

- **Prevention will fail eventually**
- Detection and Prevention are forever
- Monitoring inbound not effective
- Monitor and profile outbound traffic

Change Defenses

- Network Security monitoring
- Continuous Security monitoring
- Extrusion Detection
- Network Forensics

Protect the Data Not the Device

- Define sensitive data
 - PII, PCI, FERPA, HIPAA
- Find sensitive data
 - IdentityFinder, Find_SSN
- Protect sensitive data
 - Office Encryption, TrueCrypt, PGP/GPG
- Monitor outbound traffic



Sensitive Data Workflow

- Data Trustee (Owner) approval needed if sensitive data is involved
 - [Procurement Workflow](#)

**Nobody ever
listens to me....**





The 20 Critical Controls

- Based on ISO 27002, NIST 800-53 Standards
- Subset of Priority 1 NIST 800-53 controls

20 critical controls

Quick wins

- Focus on the most common and damaging threats
 - Consistent implementation
 - Metrics to justify acquisitions
- Interfere with
 - Attackers getting in
 - Attackers staying in
 - Attackers causing damage

Why 20 Critical Controls?

- Subset of the Priority 1 items in NIST 800-53
- 27002->800-53->20 Critical Controls
- <http://www.systemexperts.com/assets/tutorials/SystemExperts-SANS20-1.pdf>
- Technical controls only, not operational controls
- Have to start somewhere
- **Focus is ASSURANCE not compliance!**



The 20 Critical Controls: 1-3

- **1. Inventory of authorized and unauthorized devices**
 - Reduce the ability of attackers to find and exploit unauthorized and unprotected systems: Use active monitoring and configuration management to maintain an up-to-date inventory
- **2. Inventory of authorized and unauthorized software**
 - Identify vulnerable or malicious software to mitigate or root out attacks: Devise a list of authorized software and deploy tools to track software installed (including type, version, and patches)
- **3. Secure configurations for hardware and software on laptops, workstations, and servers**
 - Build a secure image that is used for all new systems deployed to the enterprise



The 20 Critical controls: 4-5

4. Continuous Vulnerability Assessment and Remediation

Proactively identify and repair software vulnerabilities reported by security researchers or vendors: Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities

5. Malware Defenses

Block malicious code from tampering with system settings or contents, capturing sensitive data, or spreading



The 20 Critical Controls: 6-7

- **6. Application Software Security**

- Neutralize vulnerabilities in web-based and other application software:

- [Vendor Application Security Questionnaire](#)

- **7. Wireless Device Control**

- Protect the security perimeter against unauthorized wireless access: Allow wireless devices to connect to the network only if it matches an authorized configuration and security profile and has a documented owner and defined business need.



The 20 Critical Controls: 8-10

8. Data Recovery Capability (validated manually)

9. Security Skills Assessment and Appropriate Training To Fill Gaps (validated manually)

10. Secure configurations for network devices such as firewalls, routers, and switches

- Compare firewall, router, and switch configurations against standards for each type of network device

The 20 critical controls: 11-13

11. Limitation and Control of Network Ports, Protocols, and Services

- Allow remote access only to legitimate users and services: Apply host-based firewalls and port-filtering and scanning tools to block traffic that is not explicitly allowed

12. Controlled Use of Administrative Privileges

- Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack

13. Boundary Defense

- Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines



The 20 Critical Controls: 14-15

14. Maintenance, Monitoring and Analysis of Audit Logs

- Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed, and activity on victim machines:. Store logs on dedicated servers, and run reports to identify and document anomalies.

15. Controlled Access Based On Need to Know

- Prevent attackers from gaining access to highly sensitive data: Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.



The 20 critical Controls: 16-20

16. Account Monitoring and Control

- Keep attackers from impersonating legitimate users: Review all system accounts and disable any that are not associated with a business process and owner.

17. Data Loss Prevention

- Stop unauthorized transfer of sensitive data through network attacks and physical theft: Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers.



The 20 Critical Controls: 18-20

18. Incident Response Capability (validated manually)

19. Secure Network Engineering (validated manually)

- Keep poor network design from enabling attackers: Use a robust, secure network engineering process to prevent security controls from being circumvented. Allow rapid deployment of new access controls to quickly deflect attacks.

20. Penetration Tests and Red Team Exercises (validated manually)

RBSM Metrics

- Reduce # of compliance violations
- Track # of staff receiving certifications
- Reduce # of user enforcement actions

Conclusions

- RBSM provides high level direction
- 20 Critical Controls provide specific areas to address
- Focus is assurance NOT compliance