

DACUM Research Chart for Information Security Specialist

DACUM Panel

Titilope Atekoja
IS Manager
Proform Industries
Columbus, OH

Joseph Gaines
Supervisor Network Systems
Columbus State Comm. College
Columbus, OH

Anderson E. Reed
General Agent/IT Specialist
Legacy Financial Solutions
Westerville, OH

Steve Romig
Senior Systems Dev./Engineer,
OSU
Columbus, OH

Chris Wilder
Compliance Manager
Sterling Commerce
Dublin, OH

DACUM Facilitators

W. Kenneth Cox
Anderson Estwick
Sheila McGrath
Christine Wagner, Team Leader

Sponsored by



Produced by



July 13-14, 2006

DACUM Research Chart for Information Security Specialist**

Duties		← Tasks →				
A	Implement Information Security Policies & Procedures	A-1 Secure management buy-in	A-2 Review existing security policies*	A-3 Review security regulatory issues	A-4 Review security "best" practices*	A-5 Write security policies
		B-1 Determine security topics (e.g. awareness, training, education)	B-2 Determine target audience (e.g., end-users, network administrators, managers)		B-3 Determine awareness media (e.g., flyers, e-mail, CBY, posterboards)	B-4 Implement awareness message
B	Implement Security Awareness Training & Education	C-1 Review network architecture for firewall implementation		C-2 Determine infrastructure requiring firewall protection	C-3 Evaluate firewall software/hardware	C-4 Purchase firewall solutions (e.g., hardware, software)
		C-11 Set up firewall paging notifications	C-12 Audit firewall rules	C-13 Perform firewall code upgrades		
C	Administer Firewall Systems	D-1 Review network architecture for IDS/IPS implementation*		D-2 Determine infrastructure requiring IDS/IPS protection*	D-3 Evaluate IDS/IPS software & hardware*	D-4 Purchase IDS/IPS solutions (e.g., Cisco, Checkpoint)
		D-12 Set up IDS/IPS paging notifications	D-13 Generate IDS/IPS reports*	D-14 Set up IDS/IPS log retention	D-15 Upgrade IDS/IPS software & attach signatures	D-16 Deploy honey pots & honey nets
D	Administer Intrusion Detection & Prevention Systems	E-1 Design network wired/wireless topology	E-2 Document network wired/wireless topology*	E-3 Implement network wired/wireless topology*	E-4 Secure network wired/wireless topology	E-5 Monitor network switches & routers*
		F-1 Configure security controls	F-2 Lockdown computer system	F-3 Install software applications (e.g., antivirus, anti-spyware, host-based intrusion detection)*		F-4 Maintain software applications (e.g., antivirus, anti-spyware, host-based detection)*
E	Administer Network Systems	G-1 Determine what to back up (e.g., computer systems, files, servers)		G-2 Determine back up software (e.g., Tivoli, Veritas)	G-3 Determine how often to back up	G-4 Determine type of back up (e.g., full, incremental)
		G-12 Incorporate back up recovery procedures into DR/BCP plan		G-13 Maintain back up software*	G-14 Maintain back up hardware*	
F	Administer Computer Systems	H-1 Identify what to log (e.g., application, systems, servers)*		H-2 Determine how to log (e.g., Syslog, Event)*	H-3 Determine log retention period*	H-4 Implement log storage system*
		I-1 Determine NOS*	I-2 Develop security policies	I-3 Set up password policies*	I-4 Identify network users*	I-5 Create user accounts*
G	Administer Back Up Systems					
H	Monitor Systems Logs					
I	Implement Identify Management					

**Although all panelists are Information Security Specialists, all panelists do not perform every task on this research chart. In addition, panelists do not necessarily perform each task in the order they appear on the chart.

NOTE: Entry level tasks are indicated by a single asterisk (*).

July 13-14, 2006

A-6 Solicit technical critique from SMEs	A-7 Coordinate review by governance groups (e.g., legal, HR)	A-8 Publish security policies & procedures	A-9 Inform end-users of security policies & procedures (e.g., flyer, e-mail)*		A-10 Enforce security policies & procedures	A-11 Coordinate internal & external audits
B-5 Determine content for training & education	B-6 Develop training materials	B-7 Evaluate 3 rd party training resources*	B-8 Perform security training	B-9 Evaluate effectiveness of security training	B-10 Determine frequency of training	B-11 Conduct annual review of security training
C-5 Install firewall	C-6 Configure firewall	C-7 Set up firewall rules	C-8 Test firewall solutions (e.g., hardware, rules fail overs)		C-9 Back up firewall	C-10 Document firewall layouts (e.g., rules, configurations)
D-5 Install IDS/IPS	D-6 Configure IDS/IPS	D-7 Set up IDS/IPS rules & thresholds	D-8 Perform network traffic analysis	D-9 Perform penetration testing of IDS/IPS	D-10 Back-up IDS/IPS	D-11 Document IDS/IPS layouts (e.g., rules, configs)*
E-6 Monitor peripheral network devices	E-7 Report on uptime & traffic statistics*	E-8 Upgrade code on switches & routers				
F-5 Install OS patches*						
G-5 Determine back up rotation	G-6 Determine capacity planning	G-7 Set up paging alerts	G-8 Implement back ups	G-9 Test back ups*	G-10 Establish off-site procedures*	G-11 Check back up logs*
H-5 Interpret logs (e.g., application, system, servers)*		H-6 Troubleshoot log failures*	H-7 Generate system reports*	H-8 Implement log monitoring & escalation*		
I-6 Create user groups*	I-7 Create access rights for user groups*					

DACUM Research Chart for Information Security Specialist

Duties		← Tasks				
J	Develop Disaster Recovery/Business Continuity Plans	J-1 Consult with systems integrator(s)	J-2 Serve on DR/BCP committee	J-3 Prioritize critical assets (e.g., data, process)	J-4 Review other DR/BCP)	J-5 Write DR/BCP proposal
		K-1 Identify systems needing to be secured*	K-2 Identify high secure areas*	K-3 Install physical security devices (e.g., anchor pads, lockable racks)*		K-4 Secure software media (e.g., Safe, Vault)*
K	Implement Physical Security	L-1 Create security panel (e.g., sys admin, communications, legal)		L-2 Identify systems compromised*	L-3 Isolate affected systems*	L-4 Consult with systems contact (e.g., administrator)*
		L-10 Perform targeted risk analysis	L-11 Determine mitigation strategies			
L	Respond to Security Incidences	M-1 Identify assets (e.g., computer, process, data)*	M-2 Determine threats to assets (internal & external)*	M-3 Calculate expected loss (e.g., reputation, income, productivity)		M-4 Identify potential mitigation strategies (e.g., firewall)
		N-1 Develop job descriptions	N-2 Review applications (e.g., resumes)*	N-3 Conduct job interviews*	N-4 Assign job tasks (after new hires)	N-5 Conduct performance reviews
M	Perform Risk Analysis	O-1 Prepare presentations/briefings	O-2 Conduct presentations/briefings	O-3 Maintain licensing records*	O-4 Set up IS/IT test labs*	O-5 Develop long range IS/IT plans
		O-11 Maintain IT/IS inventory (e.g., requisition, procurement)*		O-12 Assist with RFP development*		
N	Manage Employees	P-1 Study industry publications*	P-2 Participate in IT/IS workshops/seminars*	P-3 Participate in IT/IS continuing education*	P-4 Review IT/IS training materials*	P-5 Maintain professional certification(s) *
O	Perform Administrative Activities					
P	Pursue Professional Development					

Acronyms

OS Operating System
 IDS Intrusion Detection System
 IPS Intrusion Protection System
 DR Disaster Recovery
 BCP Business Continuity Plan
 NOS Network Operating System
 RFP Request for Proposal
 UPS Uninterruptible Power Supply
 OSI Operating System Interconnect

VOIP Voice Over Internet Protocol
 RFID Radio Frequency Identification
 GPS Global Positioning System
 VM Virtual Machine
 VPN Virtual Private Network
 IP Internet Protocol
 G Gigabyte
 SME Subject Matter Expert

J-6 Obtain DR/BCP proposal funding	J-7 Implement DR/BCP	J-8 Test DR/BCP*	J-9 Review DR/BCP*	J-10 Update DR/BCP		
K-5 Secure wiring closets*	K-6 Install security cameras*	K-7 Install access devices (e.g., keypads, keycards, biometric)*	K-8 Determine access rights*	K-9 Maintain access log book*	K-10 Coordinate with public safety on security issues (e.g., police security)*	
L-5 Perform analysis of compromised systems	L-6 Investigate other compromised systems (e.g., computers, routers, switches)*		L-7 Notify contacts of vulnerable systems*	L-8 Notify Data Disclosure Committee	L-9 Repair affected systems (e.g., disinfect or rebuild)	
M-5 Calculate cost of mitigation	M-6 Select mitigation strategy	M-7 Implement mitigation strategy				
O-6 Participate in meetings (e.g., budget, staff, project)*		O-7 Assist with IT/IS budget development	O-8 Manage IT/IS budget	O-9 Manage vendors (e.g., codes, time frames, costs, QC)	O-10 Develop procedures (e.g., network administrators, troubleshooting, help desk procedures)	

Acronyms

OS Operating System
 IDS Intrusion Detection System
 IPS Intrusion Protection System
 DR Disaster Recovery
 BCP Business Continuity Plan
 NOS Network Operating System
 RFP Request for Proposal
 UPS Uninterruptible Power Supply
 OSI Operating System Interconnect

VOIP Voice Over Internet Protocol
 RFID Radio Frequency Identification
 GPS Global Positioning System
 VM Virtual Machine
 VPN Virtual Private Network
 IP Internet Protocol
 G Gigabyte
 SME Subject Matter Expert

General Knowledge and Skills

Ethical hacking
Understanding networking protocols
Network security
Basic networking skills (e.g., OSI model)
Network topologies
Basic routing
Routing protocols
Troubleshooting skills
Managing skills
Security topology
Communication skills (e.g., presentation skills)
Project management skills
Stress management
Knowledge of network software, hardware, and peripherals
Multi-tasking skills
Problem solving
Change management skills
Time management
Decision making
Flowcharting

Tools, Equipment, Supplies and Materials

Log aggregation software
Software packages (eg “What’s Up” Gold, Stat Seeker, HP Openview)
Switches
Routers
Firewalls
Servers
Video-conferencing
Wireless devices
Palm Pilot & Pocket PCs
Intrusion detection/IPS devices
UPS
Anti-virus software
Printers, Scanners
Microfiche devices
Cable testers
Fiber testers
Hand tools (e.g., crimpers, cutters)
Network analyzers (e.g., sniffers)
Industry manuals and guides
General office supplies
Cell phones and pagers
Laptops
Projectors

Worker Behaviors

Ability to improvise
Confident
Assertive
Ability to convey complex technical information to lay people
Proactive
Able to handle pressure in challenging situations
Integrity
Motivator
Self-starter
Non-intimidating
Diplomatic
Open minded
Perseverant under pressure
Curious about how things work and why things don’t work
Professionalism
Compassionate
Empathetic
Ability to manage emotions
Responsiveness
Thirst for knowledge

Future Trends and Concerns

Knowing a better way to secure wireless technologies
Wireless technologies (e.g., 802.11n, 10G deployments)
Security awareness (e.g., social engineering)
Virtual networking
Clustering
Voice over IP
Video-conferencing
Biometrics
RFIDs (radio frequency identification)
GPS systems (global positioning)
Network standards
Better detection
IP version 6
Network posture of clients’ servers
VM ware (virtual machine)
VPN (virtual private networking)