**RAID:**

IMPORTANT NOTE: This information was copied off the Internet. Use at your own risk.

Some language may be offensive. Concept is for memorization purposes only.

*“RAID* ***0*** *– Striping”* (say it altogether), **0** Redundancy | Bl**0**ck

RAID 1 – Mirroring. Picture the 1 is a girl in mirror.

RAID 5 – 5trip1ng.  Striping with 1 in it (get it?)

Any Raid above 1 gets parity.

3- byte stripe parity then 4 block stripe parity

6 is just 5 with redundant parity stripes

**Asymmetric Algorithms:**

1. RSA        DSA                    (SA Brothers)
2. ECC        El Gamal                  (E E)
3. Diffie Hellman Knapsack  (Guy named Diffie and his Knapsack)

The Rest are Symmetrical….. and Hashes… a Good Start.

**Symmetric:** A **FISH** named **DES** had an **IDEA** on how to make **RC4** and **AES** **SAFER**.

**HASHES:** A bunch **MD**’s hanging out with **SHA**’s **HAVAL** the **RIPE**md **TIGER**s. Think crazy party with Docs, Sha’s having all the stinky tigers.

Default Answer for modern Crypto: AES (it’s used everywhere).

Digital Signatures: RSA [Real Signature Algorithm]

|  |  |  |
| --- | --- | --- |
| **ENTICEMENT** | VS | **ENTRAPMENT** |
| Tempting ‘em | VS | Tricking ‘em |
| Legal | VS | Illegal |

**Streaming Ciphers associated with Feedback**: Never pee into the wind. *Streams feeding back into your face.*

RC4 IS ONLY STREAM

**Twofish:** 128 bits – 2x 64 bit fish. 2 Fish uses 2 Fish.  A post-whitening fish and a pre-whitening fish.

**Caesar Cipher:** Caes**3R**. **3R =** 3 to the right.

Diffie-Hellman and Mr. El Gamal are sneaky poopers- *they drop DISCRETE LOGS. Discrete Log*arithmic ciphers.

**WEP**: Pronounced WEEP- because the creators weep over how insecure it is….

**WPA: TKIP** T for Temporary fix on the way to WPA2

**WP2: AES** (Default- it isn’t TKIP) and **CCMP** (*a lot like CCCP Russians. Finally keeping the Russians Out).*

**FIREWALLS:** Layer 7 Application Firewalls. Application Proxies. Level 7 Humans can make decisions. Control Active Directory. Certificates. *Certifiably Human.*

Layer 5 Firewalls.  Short Circuit- Johnny **5**. Circuit Firewalls can monitor TCP Handshakes- Robot shaking hands.

**5**tateful Firewall5.  Just like Johnny 5 they are alive. Not quite lvl 7 humans.  5’s are 5tateful and Circuit Level.  Johnny 5 was an anomaly.

Layer 3. Static Pack3t.  Static.  They are dumb turnstiles.  Locked or unlocked. All or nothing. All or No TCP, DNS.  Turnstil3s can’t stop virus because they are yuck (NYC Subway Turnstile).  They CAN stop *malformed* packets…. Turnstiles CAN stop 1500 Super Mutants (Malformed Humans).

**LAWS:**

**Due Care v Due Diligence:**  Think of a Doctors Standard of Care.  That is the care.  Diligence is the Doctors action on you.  Due Care is Research/knowledge.  Diligence is the actions. Docs act diligently.

HIPPA sounds like HEP A (medical protection law)

HITECH Hi-Tech Breaching cyborgs attacking covered associates of HIPPA.

**$**OX: Enron… ’02 shit got real. Publically traded companies: *Adequate* Financial Disclosure, *Independent* Auditors, Internal Security Controls (CI$$P Jobs). Intentional Violators are **Criminals**

**GLBA** (The HIPPA of Financial Institutions) C&I of customer data. Breach Notifications.

**SB1386**: **B**reach Notification. Breach BEACH (California)

**CFAA:** As amended Catch All for cyber-crime.  10 computers damaged is a Felony.

**ECPA:** No Wiretaps and shit…. All in the name Electronic Communications….

**PATRIOT ACT**: Not so Patriotic Reduction to restrictions in surveillance.

**PCI-DSS:** Piece a Diss? Piece a Diss shit aint no law… Pay me.

**EU Safe Harbor**: USA Companies need only *volunteer*… Volunteers to fight in Europe.

**CMM-** “Erd-MO” IRDMO. Initial, Repeatable, Defined, Managed, Optimizing.

**Forensic Evidence Steps:** IP CEA PD (Internet | CEA | Police Department)

1. Identify        Look around
2. Preserve        Don’t Step in that!
3. Collect        Now Pick it up footprint free
4. Examine        What do we have here
5. Analyze        Take a closer look
6. Presentation    See? Look what I found!
7. Decision        Well? What do you think? [jury]

**Evidence Types:**

|  |  |
| --- | --- |
| Direct Witnesses to the cops | Secondary expert witness was my 2nd choice |
| Real Knives | Corroborative back up |
| Best Contract ever! | Circumstantial proves another fact |

**Code of Ethics Canons:** Night and Day.

First 2 Canons are at night… Super Hero Status… Protecting Society and acting honorably… Jedi

Second 2 Canons are Provide and Advance… You are a techie by day.  You must follow the canons in order… Night and Day (order).  On the test answer ethical questions by order of the canons!  And in real practice. [Read the following in Robocop’s voice – Prime Directives…it helps]

1. Protect society, the commonwealth and the infrastructure
2. Act honorably, honestly, justly, responsibly, and legally
3. Provide diligent and competent service to principals
4. Advance and protect the profession

**Policies:** Mandatory High Level = Presidential.

**Program Policy Establishes Information Security Program**

Policies have an owl!

Policies- Why? Who Who What?  Like an owl asking: *Why? Who who what?* Purpose – Why | Scope – Who this covers | Responsibilities – Who does what | Compliance – What happens when you don’t comply

1. Purpose -    Why
2. Scope -        Who
3. Responsibilities-    Who
4. Compliance-     What

**Only Discretionary Policies:** Guide*lines* and Base*lines you don’t have to wait in line.* You’ll probably need management sign off to veer from Baselines.

**Risk Analysis:** The Threat of a Fire could work through the Vulnerability of no sprinklers to destroy the whole building. The building is at risk. Threat = potentially harmful source. Vulnerability = the weakness that allows the threat to do damage

Risky Titty is Vulnerable! Risk= Threat Times Vulnerability

Risk = Threat \* Vulnerability    ←Starting point. Basic.

Risk = Threat \* Vulnerability\*Impact ←When you want to add weight to the vulnerability.  For example, you want a building full of expensive stuff to be a worse loss than an empty one.  Well Impact adds weight. **Human life is infinitely irreplaceable. It trumps all.**

Risk = Threat \* Vulnerability\*Cost (simply make the impact in money)

*Sleeve Fuck (movie quote- go home and …*:  SLEAVE F:     SLE = AV\*EF

*Drinking ale leads to slaying with arrows*:         ALE = SLE\*ARO

**TCO**: To.Tal.Cost. of.owner.ship- *Its everyyy.thing.* Initial purchase of mitigating safeguard. Upfront capital, annual mx, subscriptions.  TCO of your care would be what you paid, plus cost of all repairs, gas and oil etc.

**ROI**: Return on Investment.  What you are getting back from the safeguard.

*If ale is better than tacos you made a good choice.* If ALE is > TCO you have a +ROI (not –ROI) chose a good safeguard.

In other words if TCO > ROI then bad choice.  In other other words Safeguards should be saving money. Not simply costing the company.

**Risk Management Process:** *Love is Risky, Love potion no. 9.     9 steps*

|  |  |
| --- | --- |
| 1. **System Characterization** | What do we have |
| 1. **Threat ID** | Risk = Threat\*Vulnerability  Simply Finding THREAT and Vulnerabilities. |
| 1. **Vulnerability ID** |
|  **Control Analysis** | Current and planned controls |
| 1. **Likelihood Determination** | Simply figuring what the likelihood and impact is. |
| 1. **Impact Analysis** |
|  **Risk Determination** | Doing Quantitative and Qualitative Analysis |
| 1. **Control Recommendations** | TCO, ALE and ROI oh my! |
| 1. **Results Documentation** | Document your work |

This shit was retired in 2012. But Conrad says to know it? WTF

Just rote the 9 steps if you feel you have time. DON’T ROTE MEMORIZE THIS.

**TCP/IP Model**: *3-1-1-2* | 3 layers combined, 1 lyr, 1 lyr, 2 combined

|  |  |  |
| --- | --- | --- |
| 3 | Application | Application |
| Presentation |
| Session |
| 1 | Transport | Host to Host |
| 1 | Network | Internet |
| 2 | Data-Link | Network Access |
| Physical |

**Layers of Attacks:**

**4-** *SYN 4 Fraggle…. SYN 4 Fraggle!!*

**3-** *Loki shed 3 Smurf Teardrops.*

**Biometrics Metrics:**  FRR v FAR… *2 is greater than one. 2 is a greater offense than 1.* Type 2 is False Acceptance and 1 is False Reject.

Order of BioM’s: 1. Know 2. Have 3. Are Do y*ou KNOW what you HAVE here? No? You ARE an idiot!*

**XSS v CSRF:**CSRF is the websites misplaced trust in the uSeR.  XSS is the user’s misplaced trust in the website (xSITEscripting).  The subject being mistrusted goes at the end of the sentence.

Finally got it:  XSS is when an attacker tricks a victim into unwittingly executing a code injection attack on a website. *The user trusts the website to not allow such bafoonery!*

CSRF- the website trusts that users aren’t dumb enough to fall for Social Engineer.

**Biba vs Bell-Lapadula:** Justin Biba has no integrity.  Biba is about integrity.  If you know that then Bell is Confidentiality=Keep secrets=No Read Up, No Write Down.  (Obvious when you think about it: Can’t read higher clearance stuff and can’t share with lower clearance holders).  Flip those two for Integrity=Biba: No write up no read down.

**Clark-Wilson:** *Don’t touch my shit!* Lewis and Clark telling Native Americans not to touch their stuff.  Untrusted users aren’t allowed to have access to resources without going through a protected application [web interfaces for example].

**Access Control:** MAC = Lattice – Big MAC with lattice. *Lattice is a MAC*.

Non-Discretionary = Role-Based. *Job Roles are Non-Discriminatory in USA*.

**CERTIFICATION and ACCREDITATION:** A-C-C - ACCREDITATION | ACCEPTANCE.  Accreditation is management’s acceptance of a product.  First it’s certified, then accredited (accepted) and finally implemented.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **X** | **T** | **A** | **C** | **A** | **C** | **S** | **+** |
|  | **C** |  |  |  |  |  |  |
|  | **P** |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **D** | **I** | **A** | **M** | **E** | **T** | **E** | **R** |
|  |  |  |  |  | **C** |  |  |
|  |  |  |  |  | **P** |  |  |
|  |  | **U** |  |  |  |  |  |
| **R** | **A** | **D** | **I** | **U** | **S** |  |  |
|  |  | **P** |  | **D** |  |  |  |
|  |  |  |  | **P** |  |  |  |

RADIUS is the only one that use UDP.

**Order of TACACS**.  Then a wild X appeared (we read left to right). XTACACS.  Then the X rolled behind the word to the right and landed on its side- XTACACS+.  The plus is the bonus of Multi-Factor Authentication.

**Multitasking:** Multi Multi Tasking- It allows multiple tasks to use multiple processes.

Multithreading.  Multiple. Threading = Multiplethreads at one time.  Most applications allow multithreading. Most processors allow multitasking. *When you press ALT CTRL DEL in Windows you get Task Manager… thus the CPU is running multiple Tasks.  Each app in of itself is multithreading.*

**Embedded Devices:***Cell phones are embedded in our pockets.*  It’s devices that are everywhere.

**Cyber Incident Response Life-Cycle:**

|  |  |
| --- | --- |
| 1. **P**reparation | Boy Scouts prepare first! Then this little gem:  “The PD looks in RooM’s for PreCuM Lessons with a bunch of Re-Re’s.”  ALWAYS End with a lessons learned.   * Reporting happens throughout starting at detection. * Remediation begins in Mitigation and runs parallel. No sense in waiting to fix that shit. |
| 1. **D**etection / ID |
|  **R**esponse / Containment |
|  **M**itigation / Eradication |
|  Re**P**ort |
|  Re**C**over |
|  Re**M**ediate |
|  Lessons Learned |

**Snort:** NIPS Snort NIDS ←Snort open source NIPS and NIDS

**Tripwire:** Picture a virtual tripwire into your PC.  It’s a HIDS. *For the exam HIDS (Tripwire) observes the files…. So now picture the tripwire attached to files. (Does it through Hashing FOOL!)*

**DRP/BCP**

**DRP:** *RAC AR* Respond Activate Communicate Assess Reconstitution

*Rack AR-15…*

**BCP and/or DRP Steps:** *PiSs Burp InBound! PS BIRP IB*

|  |  |
| --- | --- |
| 1. Project Initiation | Run the .ini first! |
| 1. Scope the project | Guns = Scopes = Range Fans… whats covered. |
| 1. Business Impact Analysis | **The big daddy** |
| 1. ID Preventive Controls | Prevent so you don’t need recovery |
| 1. Recovery Strategy | Prev. Ctrls didn’t catch it! We need a Recvry. Strat stat! |
| 1. Plan Design and Development | How are we going to do this? |
| 1. Implementation, Training and Testing | Lets do this! IMP TITTY |
| 1. BCP/DRP Maintenance | No Rest for the weary. |

The Piss (PS) gets its own cup.  In that cup is the .ini and scoping out what we’ll need.

The Burp (BIRP) is the BIA- we figure out what we have to protect.  Then we ID how we are going to prevent bad things. Oh shit, that didn’t work- we need a Recovery Strategy.  OK let’s get a Plan Designed and Developed to get the company ready.

The Inbound is all about the **Imp** Ti**tt**ies. **Imp**lement **T**rain and **T**est; and of course no rest for the weary… keep on it.

The .ini calls up formal guidance and authority for the project. CPPT.exe is called by the .ini.  The “Captain” aka CPPT is Continuity Planning Project Team figures who is who for the .ini.

3 Items Management Execs are responsible for in BCP/DRP:

1. Initiating
2. Final Approval
3. Demonstrate Due Care Due Diligence

*Initiate Final Demon Due Due.*

**BIA**- 2 Processes to *ultimately* find the MTD’s for specific IT Assets.

Processes:

1. ID of Critical Assets.
2. Comprehensive Risk Assessment Conducted.

\*\*These are find the MTD (RTO+WRT) of Specific IT Assets.\*\*

Now you have the MTD…. You looked at how to prevent it… now look at how to save it if un-prevented….

**Recovery Strategies**:

|  |  |
| --- | --- |
| **Redundant Site** | Instant fail over.  Site running in parallel. |
| **Hot Site** | Just shy of parallel. Less than an hour recovery. Parallel Databases and security etc. |
| **Warm Site** | 24 to 48 hours boot up time. Back-Up Data not in parallel. Hardware ready- Backups not. |
| **Cold Site** | Cheapest. No Backup data. No immediate hardware. MTD measured in weeks.  May be waiting on vendor shipments of hardware etc. |

**\*All these sites have raised floors, power, utilities and physical security\***

Other Plans:

If it’s a B plan… Business Plan… BCP or BRP then it is business focused and not IT focused.  It covers IT as a support piece to other essential Business functions.

The **COOP**.  **CO**nt. **O**p. **P**lan.  You gotta fly the coop and hide out for 30 days. Not IT focused… HQ writes it up.  So- a chicken coop full of accountants with 30 days of supplies.  30 days.

**Cont. of Support Plan aka IT Contingency Plan:** Addresses IT Disruption- Not business plan.  IT Supports ~~ hence Continuity of Support Plan.

**Crisis Commo. Plan:** Not IT Focused. Simply how to get a hold of people- Call trees.

**Cyber Incident Response Plan:** Remember PD in the RooM looking for PreCuM Lessons?  Yeah. That. And its IT Focused. Cyber Cops.

**DRP:** Often IT Focused. Major Disruptions Long term effects

**OEP (Occupant Emer.** **Plan)**: Coordinated effort to minimize loss of life and injury *and property damage* in response to a physical threat. Purely based on people.

**Crisis Management Plan:** When managers can’t communicate they go into crisis.

**BRP**:  The BURP is the relief after a disaster… going from

**DRP then BRP**:The ol’ Durp and Burp.

SO THE ONLY IT FOCUSED PLANS ARE (**CDC**):

* **C**ontinuity of Support / IT **C**ontingency Plan
* **D**RP
* **C**yber Incident Response Plan

Vital Records: SLA’s, Phone Lists, licensing info, support contracts, reciprocal agreements, etc. etc. need to be stored in hard copy and digital formats offsite.  This should be self-evident.

**Grand-Father Methodology** for Tapes = YYMMDD, Year / Month/ Day.  *Grand-Father has a Date!!* 7 Daily’s, 4 weekly, 12 Monthly.

Or Grandpa’s birthday is 7-4-12.

**Electronic Vaulting:** Big bags of money in and out…not individual bills (the big bags of money are BATCH PROCESSING)

**Remote Journaling:** Shitty Journalists keep logs not actual data. RJ sends transaction logs afar- not actual data.

**DB Shadow:** Shadows one direction under the sun. (One-way writes of DB Data to a Shadow DB)

**\*\*\*\*TESTING OF DRP/BCP SHOULD BE DONE ANNUALLY\*\*\*\*\*\*\*\***

**Walk-Through vs Walkthrough *Drill*:**A drill is an actual… drill.

**The goal of all the test are to ensure Organization Readiness**

**Security Clearances:** Private and Military

US Can Stop Terrorism: Unclassified, Sensitive, Confidential, Secret Top Secret.

TS – Grave damage        A Top Secret Grave for Jimmy Hoffa

**S** – **S**erious damage

**C**- **C**ause damage

Classified Data is C, C and above. C for Confidential. C for Classified.

Private companies use: Public, Sensitive, Confidential / Private.

Confidential- C for Company, C for Confidential… its info about company stuff versus Private which is about People info (PHI and PII for example). P for people, P for Private.

**Intellectual Property:**   Patents are 20 years from the time of patent. So-by the time a drug comes out it may only have 7 years left. *General PATENT was a great general by the age of 20.*

Copyright = Copy*write* and it is either 75 or 70 years.  Corporations get more than common people do- so Corporations 75 years from conception.  People get lifetime plus 75 years (so they actually get more).

**Gate Classes:**

1. Residential
2. Commercial
3. Industrial
4. Secure i.e. bank or airport.

*You’re looking for drugs.  First you look around the house.  Then head to Walgreens. Then you head to the plant where they make the drugs only to discover it is in a hidden vault in a bank.*

**Environmental**: Humidity is *half* the problem.  **48% ± 8**.  Temperature: *Comfortable house temps.* 68-77 or **72 ± 5**. (20-25 c).

**Fire Type Codes:**

|  |  |  |
| --- | --- | --- |
| A | Ash (Wood and Paper) | Water or Soda Acid |
| B | Boils (Gas and Oils) | Gas or Soda Acid – Never Water |
| C | Current (Electrical) | Nonconductive material such as gas. |
| D | Ding Ding (Metal) | Dry Powder |
| K | Kitchen | Wet Chemicals |

Halon never goes on your DAK!  Halon on all but D, A or K.

**Halon and its substitutes: HALON***now playing on* ***FM200****!!! This is DJ* ***FE-13***

*FE-13 is the latest Fighter Jet. The FE-13 is the safest around.*

**802.3 v 802.11**:  The 3 is a Ethernet chord uncoiling.  The 11 is rabbit ears on a Wi-Fi access point.

**Attack Method:** *Recon. Scan Foot to fingertip.  Where are they weak? Hit the weakness.*

1. Recon
2. Footprint (network map)
3. Fingerprint
4. Vulnerability Assessment
5. Attack

**Recovery v Reconstitution:**  Reconstitution = Reconstruction = New building = get the toilet in before the server. Therefore, least critical go up first.

Recovery is the opposite.  Recover the reactor. Get the cooling rods back online before the toilet.

**Swapping v Paging**: Swap whole books. Trading pages is a partial transfer.

**Software Development Cycle**

*IDIOD pronounced IDIOT. First I is .ini and second I is implementation. Last thing you do with anything is throw it away so second D is disposal.*

1. Initiation
2. Development or Acquisition
3. Implementation ------ Certification and Accreditation here.
4. Operation
5. Disposal