Ransomware and the NIST Cybersecurity Framework (CSF)

GRASSr00tz – June 9, 2022

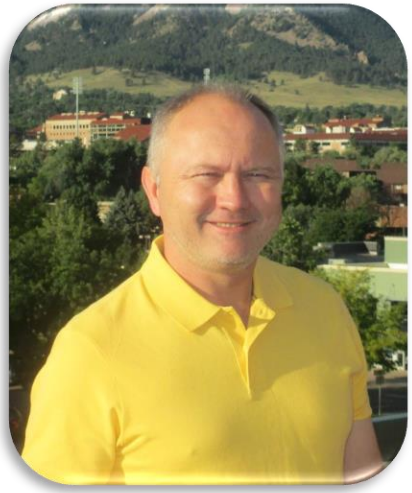
Randy Lee
https://www.randylee.com/
https://twitter.com/RandyMKE

About me (https://www.randylee.com/contact)

Current Role: Systems Engineer @ Veeam Software
Randy has led a variety of technology initiatives that have modernized legacy data centers and significantly reduced operating budgets while assuring non-disrupted operations. Randy spent over seven years as a Senior Solutions Architect at Hewlett Packard Enterprise where he was a contributing member of the Worldwide Enterprise Storage Ambassadors program for over four years. Randy has managed technology teams in manufacturing, healthcare, and the financial services industries where he focused on aligning technical strategies with corporate business objectives.

Randy has a Bachelor of Science in Business Administration/MIS with a minor in Computer Science from the **University of Wisconsin-La Crosse**. Randy is a Merit Badge Counselor for the **Boy Scouts of America**, an Auxiliary member of the **U.S. Naval Sea Cadet Corps**, and a Coach/Mentor for the **Air Force Association CyberPatriot Program**.

Randy resides with his family in the Milwaukee-Chicago area.



http://www.randylee.com

Recent Ransomware Headlines

- ✓ “EXCLUSIVE: FBI reports flood of ransomware attacks, health care companies under siege” - Washington Times
- ✓ “Several hospitals targeted in new wave of ransomware attack” - CNN
- ✓ “Ransomware hack cripples Universal Health Services hospitals, facilities across the US” – USAToday
- ✓ “Ransomware Demands Spike 320%, Payments Rise" - ThreatPost.com
- ✓ “Universal Health Services reports $67 million in losses after apparent ransomware attack” - CyberScoop
- ✓ “10K Microsoft Email Users Hit in FedEx Phishing Attack” - ThreatPost
- ✓ “WestRock Ransomware Attack Hinders Packaging Production” - ThreatPost.com
- ✓ “Ransomware gangs are now cold-calling victims if they restore from backups without paying” - VDNet
- ✓ “CD Projekt staff reportedly locked out of computers after ransomware attack” - GamesIndustry
- ✓ “Kia Reportedly Under Ransomware Attack With $20M Demand” - Motor1
- ✓ “Forward Air reveals ransomware attack, warns of revenue hit” – FreightWaves
- ✓ "Ransomware: Attacks could be about to get even more dangerous and disruptive" – ZDNet

http://www.randylee.com

Ransomware Recovery And Mitigation Costs (Estimated)

- ✓ San Miguel County, N.M. - $250,000
- ✓ Florence, Ala.- $291,000
- ✓ Tillamook County, Ore. - $300,000
- ✓ Grubman Shire Meiselas & Sacks - $365,000 (Disputed)
- ✓ La Salle County, Ill. - $500,000
- ✓ Communications & Power Industries (CPI) - $500,000
- ✓ University of California San Francisco (UCSF) - $1.14 Million
- ✓ Travelex - $2.3 Million
- ✓ **Redcar And Cleveland Council (England) - $13.6 Million To $22.2 Million**
- ✓ **Cognizant - $50 Million To $70 Million**
- ✓ **ISS World - $75 Million To $112.4 Million**

- ✓ **Post-Cyberattack, Universal Health Services Faces $67M in Losses**

Source: https://www.crn.com/slide-shows/security/the-11-biggest-ransomware-attacks-of-2020-so-far-

http://www.randylee.com

Ransomware

Ransomware is **malware** (intentionally harmful software) that employs encryption to hold a victim's information at ransom (extortion). A user or organization's critical data is encrypted. More recently, "double extortion" and "ransomware as a service (RaaS)" have become popular among threat actors.

- "On average, there is a ransomware attack every 11 seconds. 51% of victims pay the ransom at an average of $200K per attack, amounting to $20B in total cost". https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Locker Ransomware
Works by preventing system administrators from reaching their systems by denying access to computing resources, and then demanding a ransom to regain access (changing the administrator and root passwords in your corporate servers or cloud servers).

Crypto Ransomware
Works by encrypting the organization's data, taking it hostage until the victim pays the ransom and obtains the decryption key from the attacker; otherwise, data is destroyed. Crypto ransomware is the most dominant threat.

http://www.randylee.com

Ransomware

Island Hopping
Island hopping, also called leapfrogging or pivoting, is a cybersecurity exploit in which an attacker gains access to an intended target by initially exploiting the employees and supply chain partners who have access to the target's network.

In this type of **lateral attack**, the threat actor exploits a **weakness downstream** from the actual target and uses it as a launching point to reach the intended target.

Note: The term "island hopping" is inspired by a military strategy used in the Pacific theater during World War II.

Generally, island hopping attackers pick employees, customers and smaller companies that **work with the target organization**, hoping that their cyberdefense will be weaker than the ultimate target. Island hopping attacks often begin through phishing exploits in which the attacker disguises themselves as a reputable entity in an email or other communication channel.

http://www.randylee.com

Ransomware Examples

- **BadRabbit**
- BitPaymer
- Cerber
- **Cryptolocker**
- Dharma
- DoppelPaymer
- GandCrab
- Locky
- **Maze**
- MeduzaLocker
- **NetWalker**
- NotPetya
- Petya
- **REvil**
- **Ryuk**
- SamSam
- **WannaCry**

http://www.randylee.com

Ransomware Entry Points

Top Entry Points (there are more)…

- Phishing emails (most common)
- Leveraging vulnerabilities
- Remote Desktop Protocol
- Drive-by downloads from a compromised website
- USB and Removable Media

"New analysis suggests that 74% of all money made through ransomware attacks in 2021 went to Russia-linked hackers. Researchers say more than $400 million worth of crypto-currency payments went to groups "highly likely to be affiliated with Russia". Russia has denied accusations that it is harboring cyber-criminals" - https://www.bbc.com/news/technology-60378009

Вот как заставить российское ПО самоуничтожаться

Source: https://krebsonsecurity.com/2021/05/try-this-one-weird-trick-russian-hackers-hate

http://www.randylee.com

Ransomware Stages

Stage 0
Bad actors have found an entry point found. No action taken.

Stage I
Bad attackers have access to or control of an individual system or limited systems.

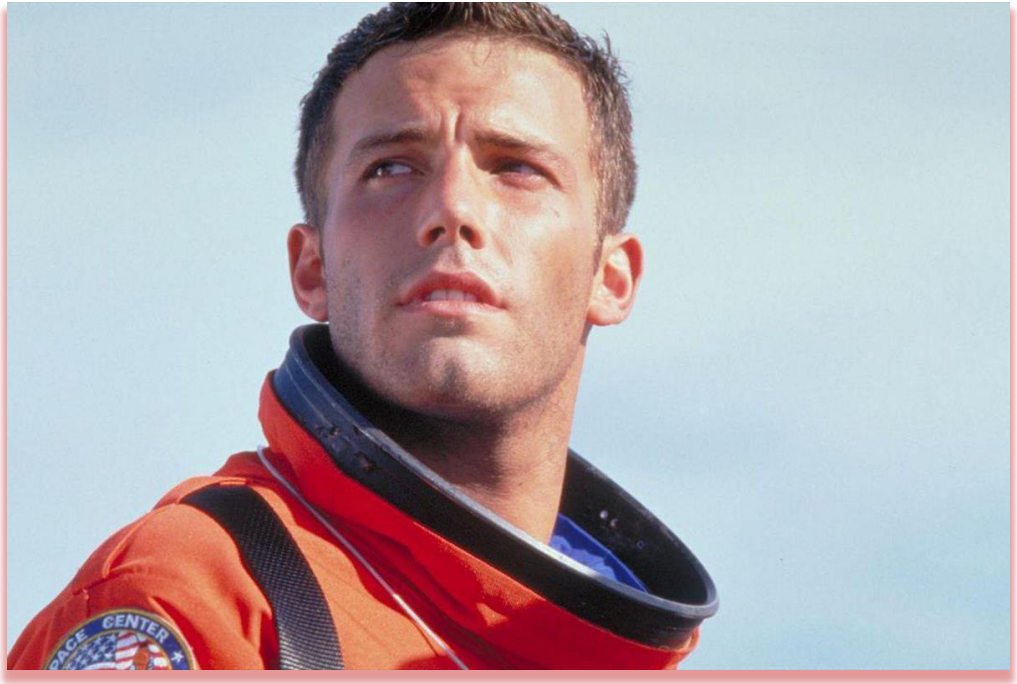
Stage II
Bad attackers have control of the broader infrastructure and are in "read-only" mode, potentially stealing data. NOTE: Dwell Time: "According to a recent SANS Institute survey, 14 percent of firms indicate that the time between compromise and detection is between one to six months." - https://threatpost.com/2021-attacker-dwell-time-trends-and-best-defenses/166116

Stage III
Bad attackers have control of the broader infrastructure and have "write" access, potentially altering data.

Stage IV
Bad attackers have administrative control. Attackers can create new means of entry as well as alter, read and steal data.

http://www.randylee.com

Speaking of BAD ACTORS…



"You know it's all funny until somebody gets shot in the leg."

http://www.randylee.com

Cybersecurity Frameworks

Cybersecurity…
Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks.

- **Due Care** – DC – "Do Correct"
- **Due Diligence** – DD – "Do Detect" (Continuous)
- Failure to demonstrate due care and/or due diligence can/will increase risk of being found negligent and/or liable for a bad event (such as a breach). When a bad thing happens, is the organization "defensible" in court?

Cybersecurity Frameworks…
Cyber security frameworks are sets of documents describing **guidelines, standards, and best practices** designed for cyber security risk management. The frameworks exist to reduce an organization's exposure to weaknesses and vulnerabilities that hackers and other cyber criminals may exploit.

There are many frameworks/standards: ISO/IEC 27001/2, NIST 800-53, **NIST Cybersecurity Framework (CSF)**, and CIS Critical Security Controls.

http://www.randylee.com

CMMC

CMMC stands for **"Cybersecurity Maturity Model Certification"** and is a unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB). DoD is migrating to the new CMMC framework in order to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB) sector.

- 17 Cybersecurity Domains

"Go" / "No Go" certification

The five levels of CMMC (1 to 5)…

1. Basic Cyber Hygiene - 17 Practices
2. Intermediate Cyber Hygiene - 72 Practices
3. Good Cyber Hygiene - 130 Practices
4. Proactive - 156 Practices
5. Advanced/Progressive - 171 Practices

http://www.randylee.com

What is NIST?

National Institute of Standards and Technology
https://www.nist.gov/

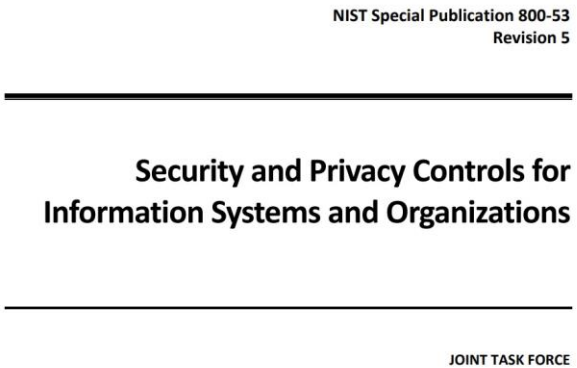
The National Institute of Standards and Technology is a
- Formerly known as "National Bureau of Standards".
- Physical sciences laboratory
- **Non-regulatory agency** of the United States Department of Commerce
- Its mission is to promote American innovation and industrial competitiveness.

"NIST helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data."
** COMMON LANGUAGE **

"NIST's activities are organized into laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement, and physical measurement."

http://www.randylee.com

NIST SP 800-53


NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for
Information Systems and Organizations

JOINT TASK FORCE

18 control families, categorized in three classes based on impact (low, moderate, and high)

"**Executive Order 13800** of May 11, 2017 - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"

NIST Special Publication 800-53 Rev 5
NIST 800-53 is **mandatory for all U.S. federal information systems** except those related to national security, and is technology-neutral. However, its guidelines can be adopted by any organization operating an information system with sensitive or regulated data.

	A	B	C
1	ACCESS CONTROL FAMILY		
2	Control Number	Control Name Control Enhancement Name	Collaboration Index Value
3			
4	**AC-1**	**Policy and Procedures**	
5	**AC-2**	**Account Management**	
6	AC-2(1)	automated system account management	
7	AC-2(2)	automated temporary and emergency account management	
8	AC-2(3)	disable accounts	
9	AC-2(4)	automated audit actions	
10	AC-2(5)	inactivity logout	
11	AC-2(6)	dynamic privilege management	
12	AC-2(7)	privileged user accounts	
13	AC-2(8)	dynamic account management	
14	AC-2(9)	restrictions on use of shared and group accounts	

http://www.randylee.com

NIST SP 800-53 – Warning: 492 Pages

process can help organizations comply with stated security and privacy requirements, obtain adequate security for their information systems, and protect the privacy of individuals.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse audience, including:

- Individuals with system, information security, privacy, or risk management and oversight responsibilities, including authorizing officials, chief information officers, senior agency information security officers, and senior agency officials for privacy;
- Individuals with system development responsibilities, including mission owners, program managers, system engineers, system security engineers, privacy engineers, hardware and software developers, system integrators, and acquisition or procurement officials;
- Individuals with logistical or disposition-related responsibilities, including program managers, procurement officials, system integrators, and property managers;
- Individuals with security and privacy implementation and operations responsibilities, including mission or business owners, system owners, information owners or stewards, system administrators, continuity planners, and system security or privacy officers;
- Individuals with security and privacy assessment and monitoring responsibilities, including auditors, Inspectors General, system evaluators, control assessors, independent verifiers and validators, and analysts; and
- Commercial entities, including industry partners, producing component products and systems, creating security and privacy technologies, or providing services or capabilities that support information security or privacy.

1.3 ORGANIZATIONAL RESPONSIBILITIES

Managing security and privacy risks is a complex, multifaceted undertaking that requires:

- Well-defined security and privacy requirements for systems and organizations;

NIST Cybersecurity Framework (CSF)

NIST Cybersecurity Framework (CSF)

- Collection of standards, guidelines, and best practices to manage cybersecurity risk.
- First published in 2014.
- **NIST CSF v1.1 is the current version** and was released in 2018.

Very comprehensive!!

In February 2013, President Obama signed Executive Order 13636, mandating that NIST develop an approach to combat cybersecurity risks against critical infrastructure.
https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636

Links…

- https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework
- https://www.nist.gov/cyberframework/framework
- https://www.nist.gov/itl/smallbusinesscyber

http://www.randylee.com

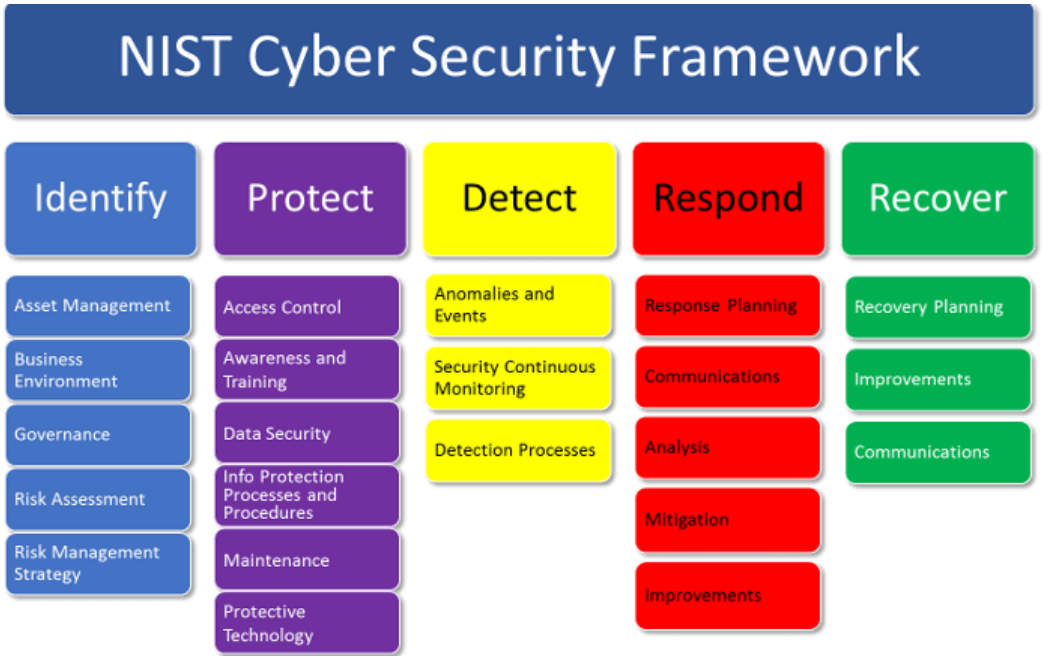
NIST Cybersecurity Framework (CSF)

NIST Cybersecurity Framework
Consists of five core functions, each with multiple subdivisions NIST calls categories. NIST CSF's five Core Functions are...

- **Identify (ID)** – 5 Subdivisions
- **Protect (PR)** – 6 Subdivisions
- **Detect (DE)** – 3 Subdivisions
- **Respond (RS)** – 5 Subdivisions
- **Recover (RC)** – 3 Subdivisions

http://www.randylee.com

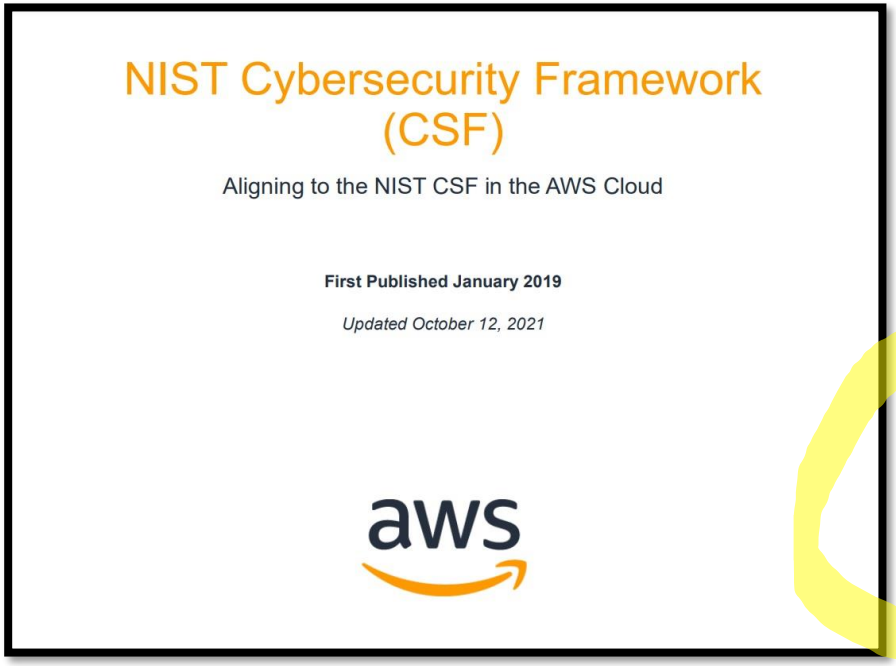
NIST Cybersecurity Framework (CSF)



NIST Cybersecurity Framework (CSF)

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST Cybersecurity Framework (CSF)



NIST Cybersecurity Framework (CSF)

Aligning to the NIST CSF in the AWS Cloud

First Published January 2019

Updated October 12, 2021

aws

Contents

CSF Identify (ID) – 5 Subdivisions

Tiers…

- Partial
- Risk Informed
- Repeatable
- Adaptive

http://www.randylee.com

CSF Identify (ID) – 5 Subdivisions

1. Maintain hardware and software inventories.
2. Document information flows.
3. Identify the external information systems to which your enterprise connects.
4. Identify critical enterprise processes and assets.
5. Establish cybersecurity policies that spell out roles and responsibilities.

http://www.randylee.com

CSF Protect (PR) – 6 Subdivisions

Tiers…

- Partial
- Risk Informed
- Repeatable
- Adaptive

http://www.randylee.com

CSF Protect (PR) – 6 Subdivisions

1. Manage access to assets and information.
2. Manage device vulnerabilities.
3. Educate and train employees and other users.
4. Protect your devices – securely.
5. Protect sensitive data.
6. Conduct regular backups.
   (This is where I spend my time).

http://www.randylee.com

CSF Protect (PR) – 6 Subdivisions

Protect…

- Always use the 3-2-1-1-0 Rule
- Management Zone - Separate Authentication Framework (Credentials)
- Leverage Immutability
- Both Encryption and Infrastructure Hardening

3-2-1-1-0 Rule - The "ZIP CODE of Availability"

- In light of the growing trend of ransomware attacks and to keep ransomware from potentially attacking your backup data first, we've modified the Backup Best Practice from 3-2-1 to 3-2-1-1-0:
- **3** - Maintain at least THREE copies of your data.
- **2** - Store critical business data on at least TWO different types of media.
- **1** - Keep ONE copy of the backups in an off-site location.
- **1** - Add another ONE to the rule where one of the media is offline (immutable).
- **0** - Ensure all recoverability solutions have ZERO errors ("Veeam SureBackup / SureReplica").

http://www.randylee.com

CSF Protect (PR) – 6 Subdivisions

Immutability

- "Immutability means that data, once written, cannot be deleted or altered for a pre-determined length of time. In the last few years, developments in encryption and security technology have made it possible to create immutable storage from ordinary computer disk drives."
  - Hardened Linux Repositories
  - Object Storage with Object Lock

- "Immutable backup of storage implies that your data is fixed, unchangeable and cannot be deleted for a period of time or sometimes, forever. Having an immutable backup is important for industries so that their data is secured from undesired accidents or circumstances."

http://www.randylee.com

CSF Protect (PR) – 6 Subdivisions

Backups vs Archives…

- **Backup**: Copy to another location in the event of data loss, damage, or corruption following an incident.
- **Archive**: Long-term data retention of inactive data that an organization needs to keep for legal or compliance reasons.

http://www.randylee.com

CSF Detect (DE) – 3 Subdivisions

DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Tiers…

- Partial
- Risk Informed
- Repeatable
- Adaptive

http://www.randylee.com

CSF Detect (DE) – 3 Subdivisions

1. Test and update detection processes.
2. Train staff.
3. Know expected data flows.

http://www.randylee.com

CSF Detect (DE) – 3 Subdivisions

Some of the following symptoms can point to an active ransomware infection in progress…

- Steady (non-bursts) increase in workload for a volume: Ransomware will likely steadily encrypt volume data. As a consequence, it will generate an increase in storage utilization.
- The added workload is approximately 50% read, and 50% write: The additional IO is likely to be well balanced between reads and writes as it reads and overwrites with encrypted data.
- The added workload has 0% compression and 0% deduplication: Encrypted data does not deduplicate or compress. A drastic reduction in DeCo efficiency or a significant increase in incremental backups size is an early warning.

❑ **"Possible Ransomware Activity"**
- CPU Usage (Warning at 70% - Error at 80%) -AND-
- Datastore Write Rate -OR- Network Transmit Rate (Warning at 40Mb/s - Error at 60Mb/s)

❑ **"Suspicious Incremental Backup Size"**
- Incremental Backup Sizes (Error at 200%)

http://www.randylee.com

CSF Respond (RS) – 5 Subdivisions

Tiers…

- Partial
- Risk Informed
- Repeatable
- Adaptive

http://www.randylee.com

CSF Respond (RS) – 5 Subdivisions

1. Develop response plans.
2. Coordinate with internal and external stakeholders.
3. Test response plans.
4. Update response plans.

http://www.randylee.com

CSF Recover (RC) – 3 Subdivisions

Tiers…

- Partial
- Risk Informed
- Repeatable
- Adaptive

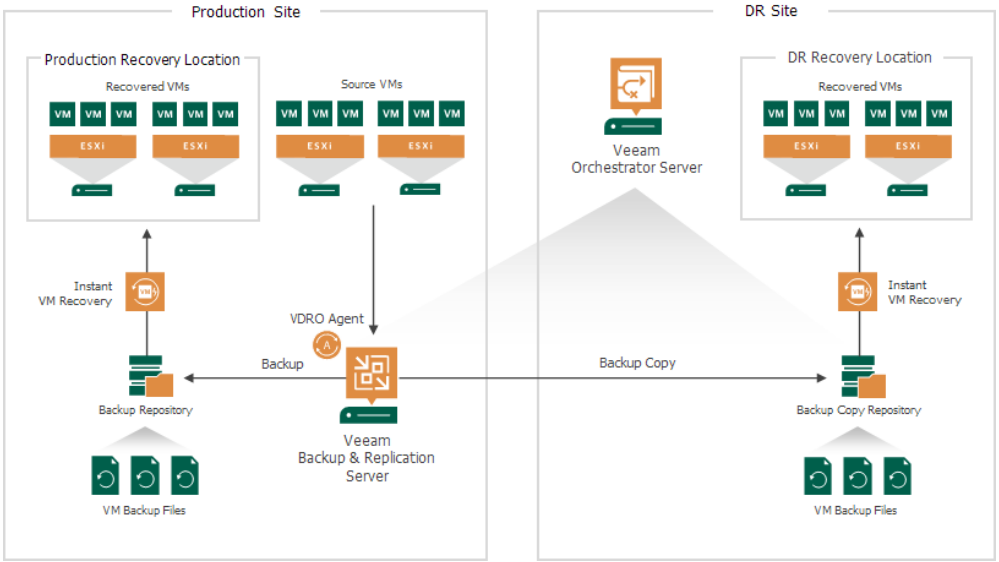
http://www.randylee.com

CSF Recover (RC) – 3 Subdivisions

1. Make contingency plans.
2. Communicate with internal and external stakeholders.
3. Manage public relations and company reputation.
4. Test and update recovery plans.

http://www.randylee.com

CSF Recover (RC) – 3 Subdivisions



"IRP - Incident Recovery Plan"

http://www.randylee.com

CSF Respond (CC)

File a Ransomware Complaint

Who should file a complaint with the Internet Crime Complaint Center (IC3)?

"You may file a complaint with the IC3 if you believe you have been the victim of an Internet crime or if you want to file on behalf of another person you believe has been such a victim."

https://www.ic3.gov/

http://www.randylee.com

Remember that RISK is...

Vulnerabilities
A vulnerability is an oversight or weakness in an organization's security posture. This could include an improperly configured firewall, an unpatched OS or unencrypted data.

Threats
A threat is something that is actually happening that the organization must defend against: DoS attack, human error, natural disasters, etc...

Risks
A risk is the careful assessment of potential threats against the organization's vulnerabilities. For example, someone stores unencrypted data in the public cloud and human error could allow the data to be accessed or changed. This could be perceived as a significant risk for the business that must be addressed.

Threats PLUS Vulnerabilities EQUALS Risk. Don't wait for the problem to be a problem!

http://www.randylee.com

Homework…

- Do you have authority (pre-authorization) to take action in the event of a cybersecurity incident?
- Do you have an IRP (Incident Response Plan)?
- **Are you interested in a TTX? *Let's chat…***

NOTE: "A tabletop exercise (TTX) for cybersecurity provides a structured opportunity to test your cooperative's ability to assess and respond to a potentially damaging cyber incident. This effort was funded by the U.S. Department of Energy to create cybersecurity resources for distribution cooperatives."

SCAN ME

http://www.randylee.com