July 2018

Security Awareness News

the security awareness newsletter for security aware people

THE RULE OF THREE

TRIADS IN UNISON

The Human Side of Security

Security: *A Delicate Balance of Triads*

Processes, People, Technology: *another powerful triad*

SECURITY:
A Delicate Balance of Triads

You may recall a beloved children's classic, The Lion King, in which Mufasa, the current king, explains to his son Simba, about how all the animals in the Serengeti are connected in the circle of life.

> ***"Everything you see exists together in a delicate balance. As king, you need to understand that balance by respecting all the creatures, from the crawling ant to the leaping antelope."***

Whether or not you are familiar with this film, these words should resonate: *a delicate balance.*

Security is not one thing. Security is not just about passwords or patching systems; it's not just incident response or intrusion detection. Security is derived through *a delicate balance* of many different elements.

Think about the triads used in the discussion of security. The CIA Triad, the foundation of the entire security industry, requires a balance of **confidentiality, integrity, and availability**. The Domains Triad encourages us to think about security in the **cyber, physical, and people** domains—not just one, but all three. The Many Lives Triad reminds us about security all around us: **at work**, **at home**, and **when we are mobile**.

Security can never be whittled down to include just one segment of our lives or just one part of a triad. A security based mindset is essential in order to keep all those segments balanced no matter where we are.

CIA Triad – *the bedrock of information security*

Confidentiality – Keeping secrets secret
Integrity – Maintaining accuracy
Availability – Ensuring the accessibility of data/systems

Domains Triad – *the three main areas or types of security*

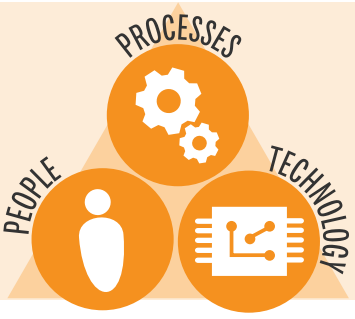
Cyber – protecting our connected computers, devices, and networks
Physical – securing tangible elements from tangible threats
People – protecting the individuals we interact with every day

Many Lives Triad – *the intersection of daily security efforts*

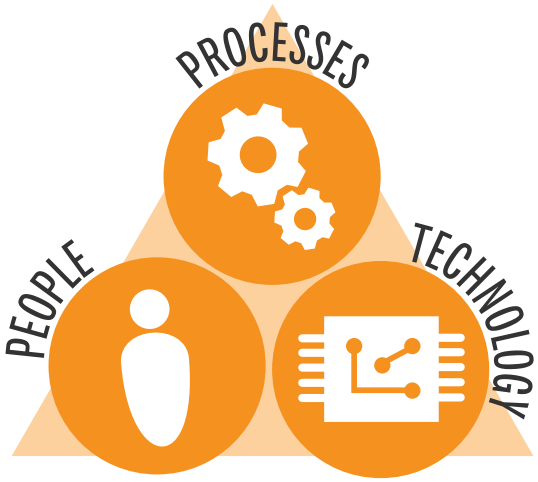
Personal – security at home, at school, with family, friends, etc.
Professional – security at work
Mobile – security on the go, whether for personal or for business

Organizational Triad – *balancing security efforts for everyone within our organization*

Processes – the procedures that help guide our efforts
People – the individuals that contribute to our efforts
Technology – the tools that offer technical solutions to enhance our efforts



Processes, People, Technology:
another powerful triad



Every organization needs to consider three fundamental components when creating a successful culture of security: Processes, People, and Technology. Too often, we get caught up in the exciting promises of purely technological solutions. ***Stop criminal hackers today! Prevent data breaches from ever happening! All of your data, 100% secure!***

We can never have a 100% guarantee of security, and to rely solely on technology would be foolish. Sure, we need to leverage technological tools to defend our networks, patch our systems, manage our passwords, encrypt our communications, and create myriad detection and defensive positions between us and those who may work hard to break through our barriers. But we must also have meaningful policies and processes in place to guide our actions, to test our systems for weaknesses, to mitigate incidents, and to let us do our jobs effectively.

Finally, we can't forget the human side of security: It is people, after all, who use the technology and follow the policies. And if we're not paying attention, we won't recognize that those same people will still click on phishing links, incorrectly configure security settings, make careless mistakes with sensitive data, or lose their mobile devices, because they ARE human, imperfect people.

Remembering to maintain that somewhat delicate balance of technology, policies, and people, as opposed to leaning too heavily on any point of the triad, will always strengthen our defenses.

Security Awareness in Action

Imagine the following scenarios and how you would handle each one. Even if they don't apply specifically to your particular position or job function, you will enhance your own situational awareness within any domain, anywhere, anytime, simply by going through the mental exercises of ***"what if?"***

1. You notice a service/repair technician accessing a controlled area of our building, without an escort:

- **A. Don't bother him. He's here to fix something.**
- **B. Ask him if he needs help finding anything.**
- **C. Ask him for credentials and check with, or report to, the designated security team point of contact to confirm that he belongs there.**

2. You receive a phone call from the IT department asking you to verify your computer login so they can run an important update:

- **A. Politely decline and report the call to the security team or your supervisor.**
- **B. Tell the caller that you'll email the login credentials since you can't verify anything over the phone.**
- **C. Verify your login because updates are a crucial part of security.**

3. You receive a text message warning you that your bank account has been locked due to fraudulent activity and instructing you to click on a link to fix it immediately:

- **A. Click the link to fix your account.**
- **B. Delete the text and call your bank directly.**
- **C. Forward the text to a friend and get their opinion.**

ANSWER KEY

1. C: There will obviously be those times when repair or maintenance work is needed, but never assume that an unfamiliar person, who is carrying tools, or wearing an appropriate uniform, actually has the clearance to access secured areas of our organization.

2. A: Avoid giving away sensitive data over the phone, unless you can 100% verify who's on the other end and they have a right to know. And always report suspicious incidents like this one.

3. B: This sounds like a social engineering attack called smishing (SMS phishing). As always, think before you click and when in doubt, contact your bank directly.

The Human Side of Security

Even with the most advanced technology in the world, our security posture is dependent upon a culture of security-aware individuals. This means that everyone here at work **(including you!)** must play their part in bolstering our organization's defenses. From the C-suite to the front desk, we all shoulder the responsibility of staying alert and using common sense in our day-to-day operations.

5 Things You Can Do Today to Strengthen Resilience to Cybercrime

(choose your role)

User

A person who helps keep our organization running on a daily basis and represents one of the most important elements of cybersecurity.

- **Always follow policy.**
- **Treat requests for sensitive info with skepticism.**
- **Know how to report security incidents.**
- **When in doubt, please ask.**
- **Develop a security policy for your personal life.**

IT/Tech/ Developer

A person in charge of developing, implementing, and managing our infrastructures and defensive strategies from a technical standpoint.

- **Keep systems up to date.**
- **Use caution when seeking help from online communities.**
- **Avoid allowing shared accounts or logins.**
- **Keep permissions restricted and document everything.**
- **Mitigate risky behavior.**

Executive/ Management

The top-level members of our organization who oversee our entire operation.

- **Lead by example.**
- **Participate in awareness training.**
- **Understand that you are a top target.**
- **Avoid oversharing on social media.**
- **Foster a culture of trust and communication within the organization.**

No matter your role, remember that security is a team sport! Every individual's effort, big or small, to protect our organization, contributes to our security-aware culture.

TRIADS IN UNISON

For decades, the CIA Triad has represented the foundation of information security; confidentiality, integrity, and availability work together to create the solid security framework of any organization. Similarly, the Many Lives Triad highlights the need for awareness in our personal, professional, and mobile lives. By combining these two triads, and identifying how and where they overlap, we can better visualize what it means to be a strong human firewall!

	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
PERSONAL	Guard your online accounts with unique passwords.	Consider encrypting your hard drives and devices.	Run regular backups of personal files such as tax info and pictures.
PROFESSIONAL	Always follow policy. Know and understand data classification.	When transferring sensitive info, ensure that it's accurate and verify the recipient.	Respect the access you've been granted. Never let someone else use your credentials for any reason!
MOBILE	Use caution when connecting to public networks.	Keep your devices up to date.	Enable remote access so you can track and wipe your device if it gets lost or stolen.

The above chart is a simplified look at the relationship between the CIA, Many Lives, and Domains Triads. Choose ANY security issue you can think of; say, phishing scams, a lost device, or a USB-connected hard drive hanging over the edge of a desk in the office. Then see which tips apply. You will soon realize that security issues are not isolated but are some combination of these three triads.