SUMMARY CYBER CIRCLE 3
– ME, IN A CRISIS

Chief Information Security Officers (CISOs) play a critical role in safeguarding an organization's digital assets and ensuring its resilience against cyber threats. Given the increasing frequency and sophistication of cyberattacks, CISOs often find themselves at the forefront of crisis management. Understanding their personality traits and stress profiles in such situations is vital to appreciating how they navigate these high-pressure scenarios.

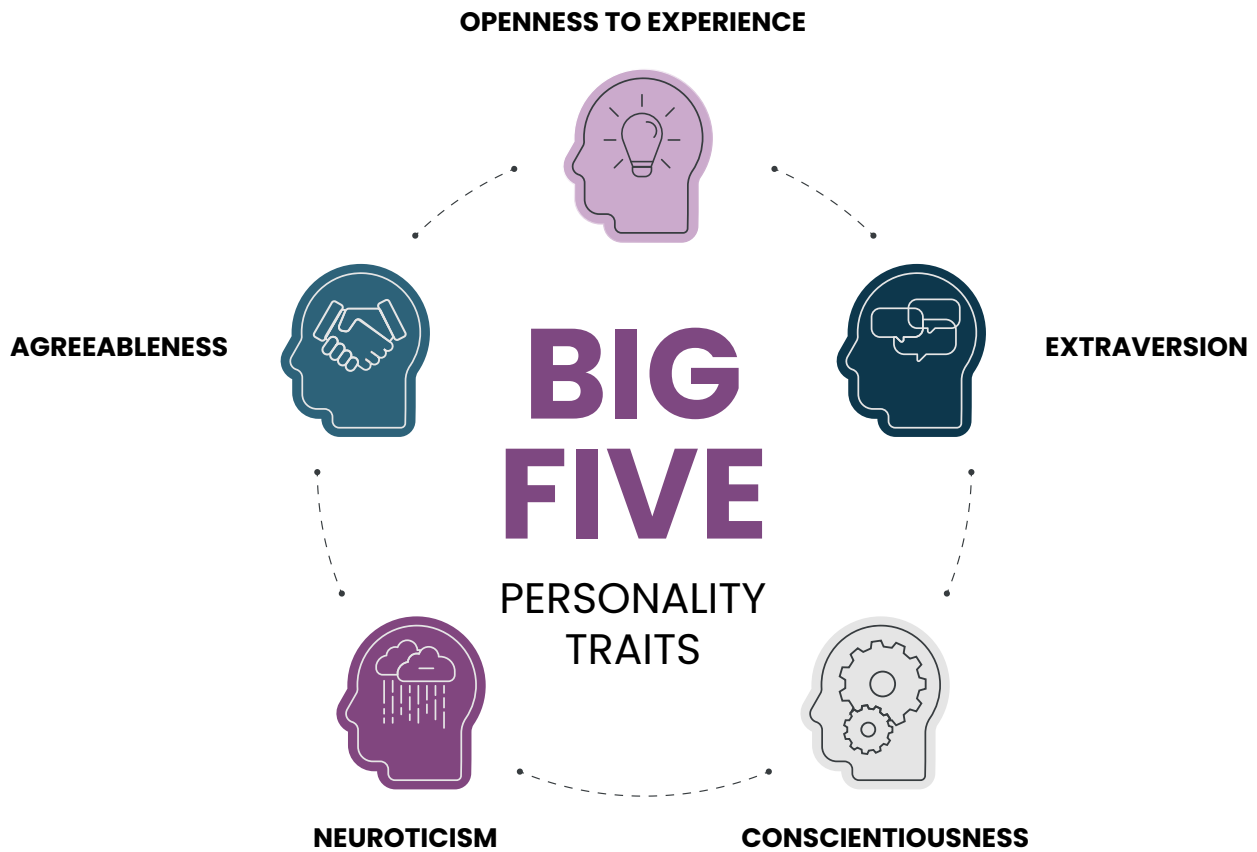**The eight dimensions of stress and their influences on a stressful situation:**

- Intensity: The severity of the stressor.
- Duration: How long the stressor persists.
- Frequency: How often the stressor occurs.
- Predictability: The extent to which the stressor can be anticipated.
- Controllability: The degree of control one has over the stressor.
- Proximity: The physical or emotional closeness to the stressor.
- Ambiguity: The clarity or uncertainty associated with the stressor.
- Complexity: The number of interconnected elements and complications within the stressor.

Stress impacts us in various ways and many of the symptoms can be encountered in crisis situations:

- Physical: e.g., sweating, difficulty to sleep
- Psychological/Emotional: e.g., anger, nervousness
- Cognitively: e.g., forgetting things, difficulty to concentrate
- Behavioral: e.g., changed eating or sleeping behavior

THE PERSONALITY IN A CRISIS

An individual's personality traits are relatively stable and influenced by genetics (ca. 50-80%) and early life experiences. Personality impacts behavior across situations, including crisis.. **Tests based on the five-factor model of personality provide good indications of an individual's personality traits.**

OPENNESS TO EXPERIENCE

AGREEABLENESS

BIG FIVE
PERSONALITY TRAITS

EXTRAVERSION

NEUROTICISM

CONSCIENTIOUSNESS

Make the test

Low Expression	Big 5 (Five-Factor Model)	High Expression
←		→
pragmatic, conservative	Openness	creative, risk-taking
spontaneous, flexible	Conscientiousness	reliable, organized
reflective, reserved	Extraversion	energetic, sociable
skeptical, competitive	Agreeableness	empathetic, cooperative
calm, emotionally stable	Neuroticism	sensitive, anxious

HELPFUL PERSONALITYTRAITS DURING A CRISIS

Trait	Relevance	Description
Openness	✔	flexible, loves new experiences
Conscientiousness	✘	
Extraversion	✔	self-assured, communicative
Agreeableness	✘	
Neuroticism	✘ ✘ ✘	insecure, anxious

Here are four personality-related aspects that are especially helpful in a crisis:

1. **Resilience:** The ability to recover quickly from difficulties and maintain a positive outlook despite challenges. This trait enables individuals to withstand and bounce back from stressful situations effectively.
2. **Decisiveness:** The capacity to make quick, informed decisions without hesitation. This is crucial in crisis situations where timely actions can mitigate further damage.
3. **Calmness under Pressure:** Maintaining composure and clear thinking when under stress. This trait helps in preventing panic and ensuring that rational decisions are made during a crisis.
4. **Effective Communication:** The ability to convey information clearly and efficiently. Good communicators can ensure that all stakeholders are informed, aligned, and working towards a common goal during a crisis.

While a significant portion of personality is relatively stable due to genetic and early environmental influences, it is not entirely fixed. People can and do change, especially in response to significant experiences and through intentional efforts, e.g., supported by mental training or psychotherapy. This balance between stability and adaptability is what makes personality both predictable and capable of growth.

HOW TO BUILD MORE RESILIENCE

STEP 1: RISK ATTENTION

In the pursuit of raising risk attention and fostering risk awareness, engaging stakeholders necessitates a structured approach:

1. CISO elucidates the broader context and interconnections of risks, aligning them with stakeholders' priorities.
2. CISO addresses stakeholders' business and personal needs to ensure relevance and resonance in risk discussions.
3. Collaboratively, stakeholders and the CISO develop a shared set of early indicators to detect and preempt risks effectively.

This systematic dialogue not only amplifies risk awareness but also bolsters organizational resilience

STEP 2: PSYCHOLOGICAL SAFETY

The concept of psychological safety refers to the belief that one is safe to take risks, make mistakes, and express themselves without fear of negative consequences. Here's how it can help increase stability and resilience in a crisis:

1. Enhanced Trust and Collaboration: When team members feel psychologically safe, they are more likely to trust one another and collaborate effectively. This trust fosters open communication, which is crucial during a crisis for swift decision-making and problem-solving.
2. Improved Problem-Solving: Psychological security encourages individuals to voice their ideas and concerns without fear of judgment. This openness leads to diverse perspectives and innovative solutions, which are vital for navigating complex crises.
3. Increased Adaptability: In a psychologically secure environment, individuals are more willing to adapt to changing circumstances. They are less likely to be paralyzed by fear of failure and more inclined to experiment with new approaches, enhancing the team's ability to respond to unforeseen challenges.
4. Emotional Stability: Feeling psychologically safe reduces anxiety and stress, helping individuals maintain emotional stability. This stability enables clearer thinking and better decision-making under pressure.
5. Resilience Building: A secure environment supports learning from mistakes and setbacks. By viewing failures as opportunities for growth, individuals and teams build resilience, becoming more capable of bouncing back from future crises.
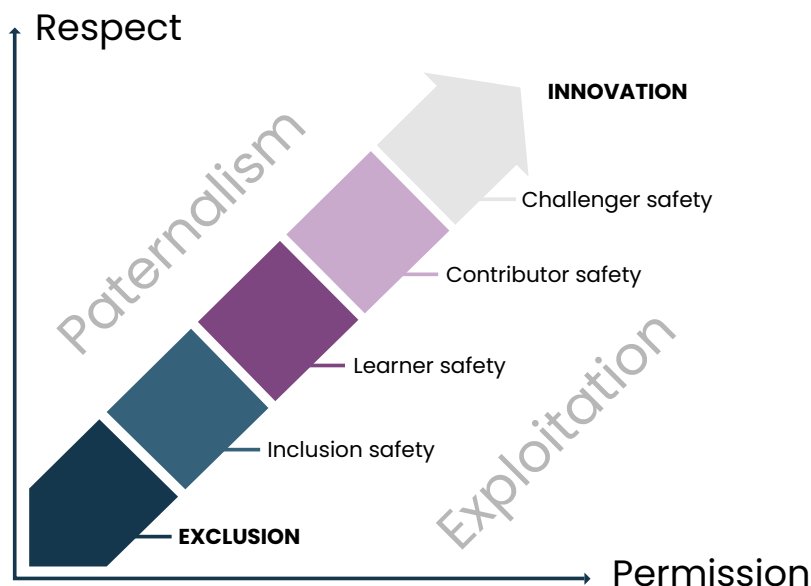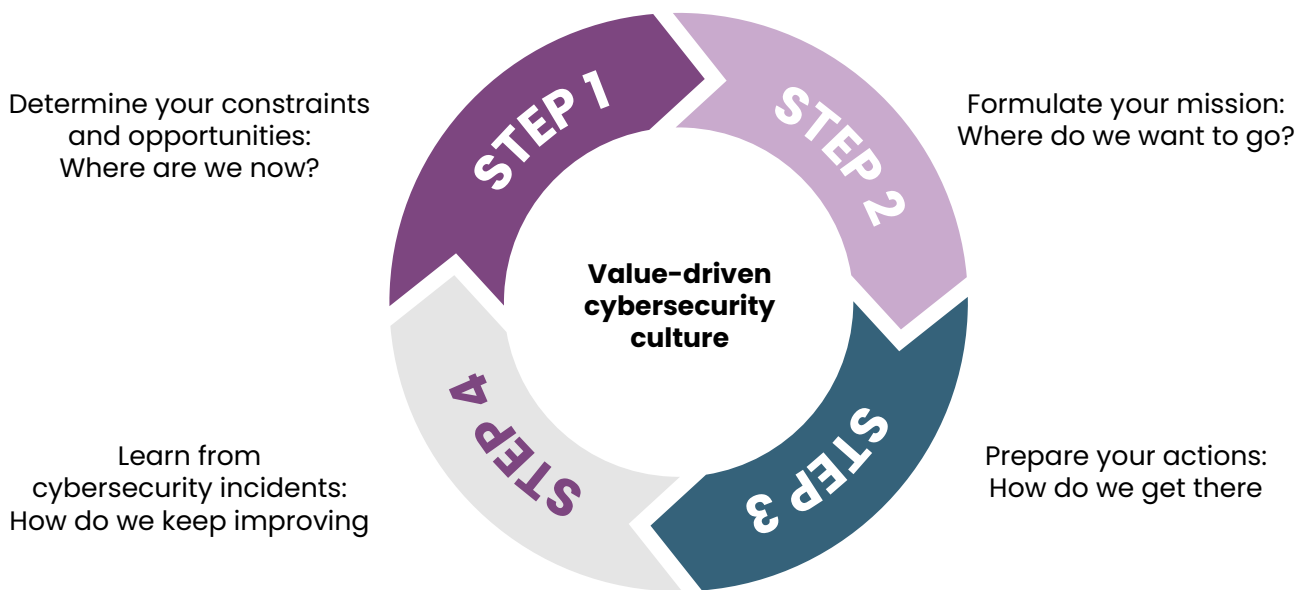

To create psychological stability during a crisis, the top stakeholders to focus on could be:

- **SOC Team (Security Operations Center Team):** This team is on the front lines of managing and responding to the crisis. Ensuring they feel secure and supported is crucial for effective and efficient crisis management.
- **Crisis Management Team:** This group coordinates the overall response to the crisis. Their ability to function smoothly and confidently under pressure is vital for the organization's stability.
- **Internal/External Communication Team:** These individuals manage the flow of information both within the organization and to the public. Psychological security here ensures clear, consistent, and accurate communication, which is essential to prevent misinformation and maintain trust.
- **CEO:** The CEO's leadership and demeanor significantly impact the organization's morale and stability. Providing psychological security to the CEO helps them lead effectively and instill confidence throughout the organization.
- **CTO (Chief Technology Officer):** The CTO plays a critical role in addressing technical challenges during a crisis. Ensuring their psychological stability helps in making sound technical decisions and maintaining the integrity of the organization's technological infrastructure.

The Chairman of the Board should also be on the radar for psychological crisis management because their leadership and decisions significantly influence the organization's strategic direction and stability.

STEP 3: CORPORATE & CYBER SECURITY VALUES

Determine your constraints and opportunities: Where are we now?

Formulate your mission: Where do we want to go?

STEP 1

STEP 2

Value-driven cybersecurity culture

STEP 4

STEP 3

Learn from cybersecurity incidents: How do we keep improving

Prepare your actions: How do we get there

Having a robust set of values embedded in a company's culture and crisis planning is instrumental in navigating challenges effectively. Here's how:

1. **Guiding Principles:** Values serve as guiding principles, anchoring decision-making processes during both normal operations and crises. When faced with uncertainty or adversity, these values provide a moral compass, ensuring that actions align with the company's ethos.
2. **Employee Alignment:** A value-driven culture fosters alignment among employees, promoting unity and coherence in crisis response efforts.
    When everyone shares common values, it becomeseasier to rally together, collaborate, and work towards common goals, even in the face of adversity.
3. **Ethical Conduct:** Values act as a safeguard against unethical behavior, especially in high-stress situations. By prioritizing integrity, honesty, and transparency, companies can maintain trust with stakeholders and navigate crises with credibility and integrity.

Here are examples of values that are particularly helpful in crisis situations:

1. **Integrity:** Upholding honesty, transparency, and ethical conduct in challenging circumstances.
2. **Empathy:** Showing understanding, compassion, and support for those affected by the crisis.
3. **Teamwork:** Collaborating effectively to address challenges and achieve common goals.
4. **Accountability:** Taking ownership of actions, accepting responsibility, and striving for improvement.
5. **Communication:** Maintaining clear, timely channels to keep stakeholders informed and manage expectations.
6. **Trust:** Building and maintaining trust through consistent actions and reliability.
7. **Safety:** Prioritizing the health and well-being of employees, customers, and communities.

STEP 4: ENHANCE STRESS MANAGEMENT SKILLS

Here are the three key strategies to enhance stress management skills and build a better stress personality:

1. **Matching:** Build a team that complements your personality weaknesses. Surrounding yourself with individuals whose strengths counterbalance your weaknesses creates a more resilient and effective team dynamic during a crisis.
2. **Training:** Engage in targeted training to develop necessary skills. This includes mental training, coaching, and self-reflection, which enhance your ability to manage stress and perform under pressure.
3. **Decrease Insecurities and Unexpected Elements:** Reduce uncertainties by thorough preparation. Training and simulation exercises help mitigate unexpected elements in a crisis, increasing confidence and control.

These strategies collectively enhance your ability to handle stress by leveraging team strengths, improving personal capabilities, and minimizing unpredictability.

CONCLUSION

In the field of cybersecurity leadership, the Chief Information Security Officer (CISO) must go beyond technical expertise to include proactive crisis preparedness in their role.

1) **Creating psychological safety is crucial, ensuring that stakeholder teams, security teams, and crisis teams feel secure to express concerns and ideas. This approach should also foster a security culture where all employees feel safe to discuss security issues.**
2) **CISOs must stay informed about evolving threats and industry best practices while cultivating strong relationships with key stakeholders. Collaborative efforts with peers in developing comprehensive crisis response plans are essential, supplemented by regular training and simulation exercises. Agility and adaptability are emphasized, with a focus on continual refinement of plans to align with emerging threats and organizational needs.**
3) **Investing in personal development, particularly in leadership and communication skills, also bolsters the CISO's ability to navigate crises effectively.**

Through these proactive measures, CISOs and their peers can fortify their organizations against cyber threats and crisis situations.

Cyber Circle, located in Switzerland,
is a project that connects CISOs
(Chief Information Security Officers)
with researchers. This collaborative
community meets every two months
for an evening of valuable discussions
and activities centered around their
roles. The focus is on providing insights,
facilitating cross-industry learning,
enabling external peer networking,
and conducting practical workshops.
The ultimate goal is to establish
improved cybersecurity principles,
including human-centered security,
within companies.

**Join Cyber Circle and become part
of a friendly community shaping the
future of cybersecurity!**

Circle hosts:
Milena Thalmann, White Rabbit Communications
Stefan von Rohr, Peer Consult
Peter Kosel, cyberunity