(BUFFY)2

2021

COLLAPSE-OLOGY

WHY EXPOSED RDP ISN'T YOUR BIGGEST THREAT

@ERRBUFFEROVERFL

https://errbufferoverfl.me
gemini://gemini.errbufferoverfl.me
merrymet@errbufferoverfl.me

COLLAPSOLOGY

WHAT THE HECK IS THIS?

noun

the transdisciplinary study of the risks of collapse of industrial civilisation.

CASE STUDY #1:

NEO-ASSYRIAN EMPIRE

7TH CENTURY BCE

LOCATION: THE NEAR EAST

IMAGE SOURCE: NINGYOU WORK DATA FROM BASED ON A MAP IN 'ATLAS OF THE BIBLE LANDS', C S HAMMOND & CO (1959), ISBN 9780843709414.

REASON FOR COLLPASE

Political Threats

- King Ashurbanipal died in 631 BC which sparked on going civil war
- This resulted in a power imbalance that allowed vassal states to began fighting back
- Documented accounts that royals experienced ongoing fears in the monarch about internal threats and rebellion

IMAGE SOURCE: BAS-RELIEF OF ASSYRIAN SOLDIER MESOPOTAMIA 1500-539 BC GALLERY, BRITISH MUSEUM, LONDON, ENGLAND, UK. COMPLETE INDEXED PHOTO COLLECTION AT WORLDHISTORYPICS.COM.

IN THE MODERN DAY

Political Threat #1: Turf Wars

When managers or employees engage in competition for bureaucratic control, resources or the advancement of individual or organisational goals and objectives.

Outcome

Security becomes a mechanism by which people fight for turf and the organisation's overall protective posture can be impaired, sometimes severely.

IN THE MODERN DAY

Political Threat #2: Vendor Bias

When individuals or groups within the organization decide on particular products, technologies, or vendors based on political motives.

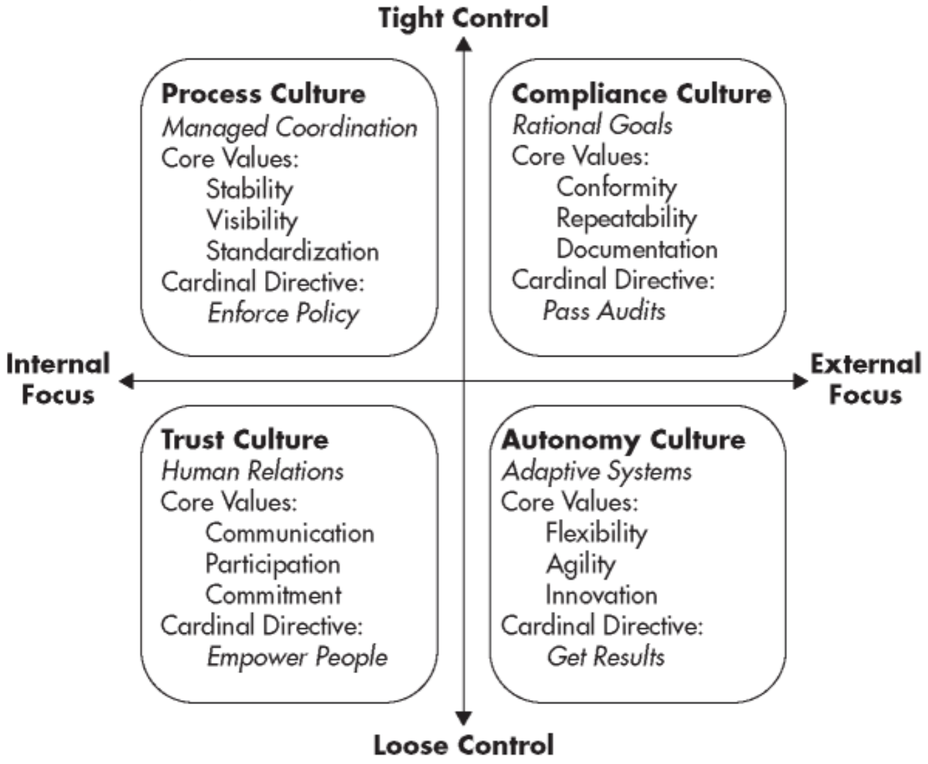
Outcome

An organisation devoting resources and engineering effort to make technology match requirements / Security teams may find themselves behind the curve on skills and innovation by supporting vendors out of a sense of loyalty.

SECURITY TOOL #1

Competing Security Cultures Framework

- A modern day remix of the Competing Cultures Framework created by Cameron and Quinn which identifies four different types of organizational culture. The four cultures they define are: hierarchy, clan, ad-hocracy and market
- The security variation was created by Dr. Lance Hayden and breaks security culture into four cultures: process, complaince, trust and autonomy cultures
- Enables you to describe and interpret the different ways that security is understood and practiced by coworkers
- Used to identify areas where competitive principles and values have emerged that may represent risk to the organisation's security goals and objectives



CASE STUDY #1

Summary

- Political threats can result in security becomes a mechanism by which people fight for turf and the organisation's overall protective posture can be impaired, while political factors that impact vendor selection can leave security teams underskilled and looking after impractical security tools
- You can use the Competing Security Cultures Framework to describe and interpret the different ways that security is understood and practiced by coworkers which can help you identify trends that suggest political stressors

CASE STUDY #2:

THE ROMAN EMPIRE

15TH CENTURY CE

LOCATION: SOUTHERN EUROPE

IMAGE SOURCE: THE ROMAN EMPIRE (RED) AND ITS CLIENTS (PINK) IN 117 AD DURING THE REIGN OF EMPEROR TRAJAN.

REASON FOR SUCCESS

High Reliability Empires

- They maintained a complex society, but also maintained healthy respect for complexity and unpredictability and invested in social programs to help equalize some of the issues created by this
- After some time Roman Empire saw an eventual redistribution of wealth and power, and this diffusion of the Republic's more rigid hierarchies led to increased social mobility -- which allowed the empire to be influenced by people close to problems.

IN THE MODERN DAY

High Reliability Organisations (HROs)

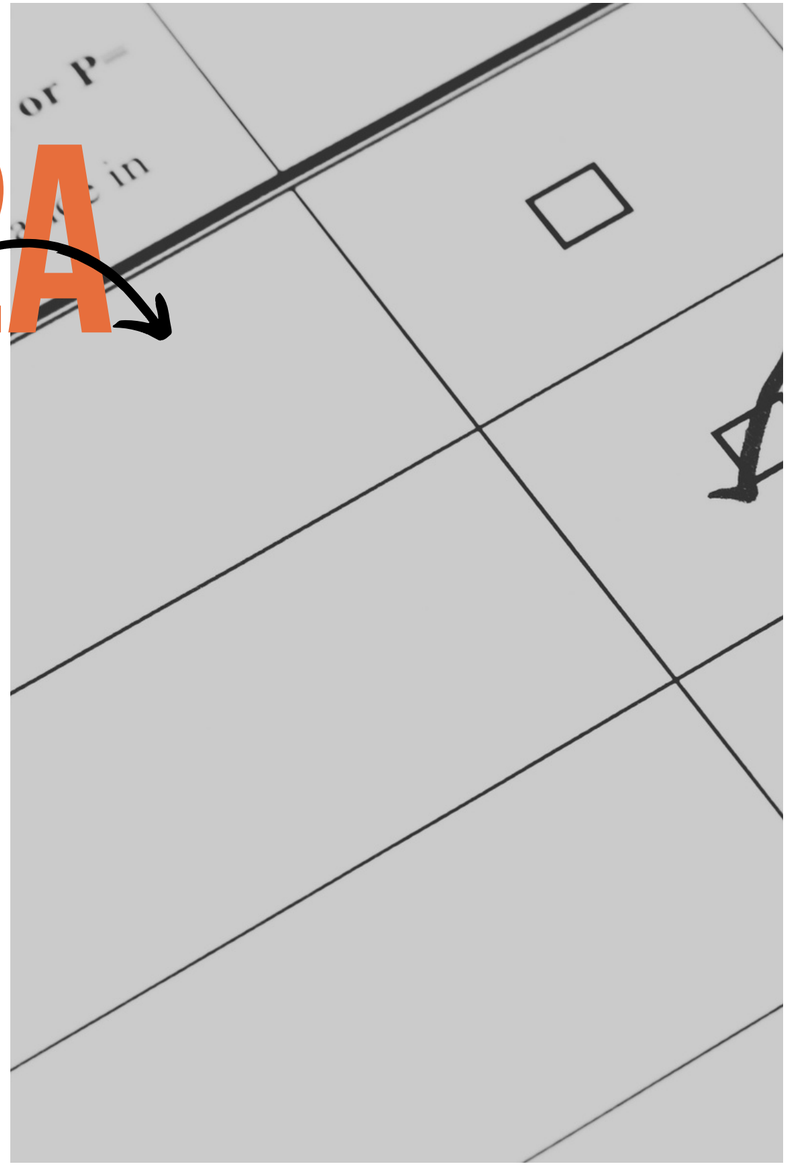
- Preoccupation with Failure: Use small frequent controlled failures to as a tool that can be used to avoid large disasters
- Reluctance to Simplify: Maintain a healthy respect for complexity and unpredictability and support this with data and metrics
- Sensitivity to Operations: Ensure that operations are accounted for and have a well defined roadmap that outlines the how, using data to link strategy and operations

IN THE MODERN DAY

High Reliability Organisations (HROs)

- Commitment to Resilience: Put effort into imagining how failure will occur and how you can get back up on your feet
- Deference to Expertise: Create deep feedback loops and seek opinions from the people closest to the problem

SECURITY TOOL #2A



Security FORCE Behavioral Model Survey

- 25 statements broken up into five key values:
  - The security value of failure
  - The security value of operations
  - The security value of reliability
  - The security value of complexity
  - The security value of expertise
- The Security FORCE Behavioural Model is generalist tool, suitable for a variety of situations and audiences
- Scoring is relatively simple as well:
  - An average score over 4 means the organisation exhibits qualities of a HRSP
  - An average score of 3 means may or may not behave like an HRSP
  - 2 or below means the organisation does not behave like an HRSP

SECURITY TOOL #2B

Security FORCE Behavioral Model Metrics

- The metrics are used to support, verify, and validate Security FORCE behaviours within the organisation it's beneficial to chart changes over time so you can graph progress and identify regressions in existing metrics:
- There are 5 metrics for each value expressed by high reliability security programs. Metrics can also be appended, removed and adapted for your organisation as it grows and changes, but the base set comes with some of the following:
  - Number of security failure scenarios developed in the past year
  - Ratio of security incidents with no prior failure reporting or indicators in the past year
  - Number of security-related training opportunities provided to people, by role or group, in the past year
  - Average time to organisational decisions (from initial proposal, through debate, or deliberation, to final resolution)

CASE STUDY #2

Summary

- High Reliability Security Programs are less about how organizations succeed at security and much more about how they fail at it, in very particular ways, under specific circumstances. They also expect to fail so they prepare for the eventuality in a way that allows them to rebound quickly and gracefully from a fall
- You can use the Security FORCE Behavioral Model Survey & Metrics to help change the habits and behaviours in a security and to adopt new ones that will not only make large failures less likely, but enable better responses to those that inevitably do occur

CASE STUDY 3:

THE MODERN DAY

21ST CENTURY CE

LOCATION: HERE

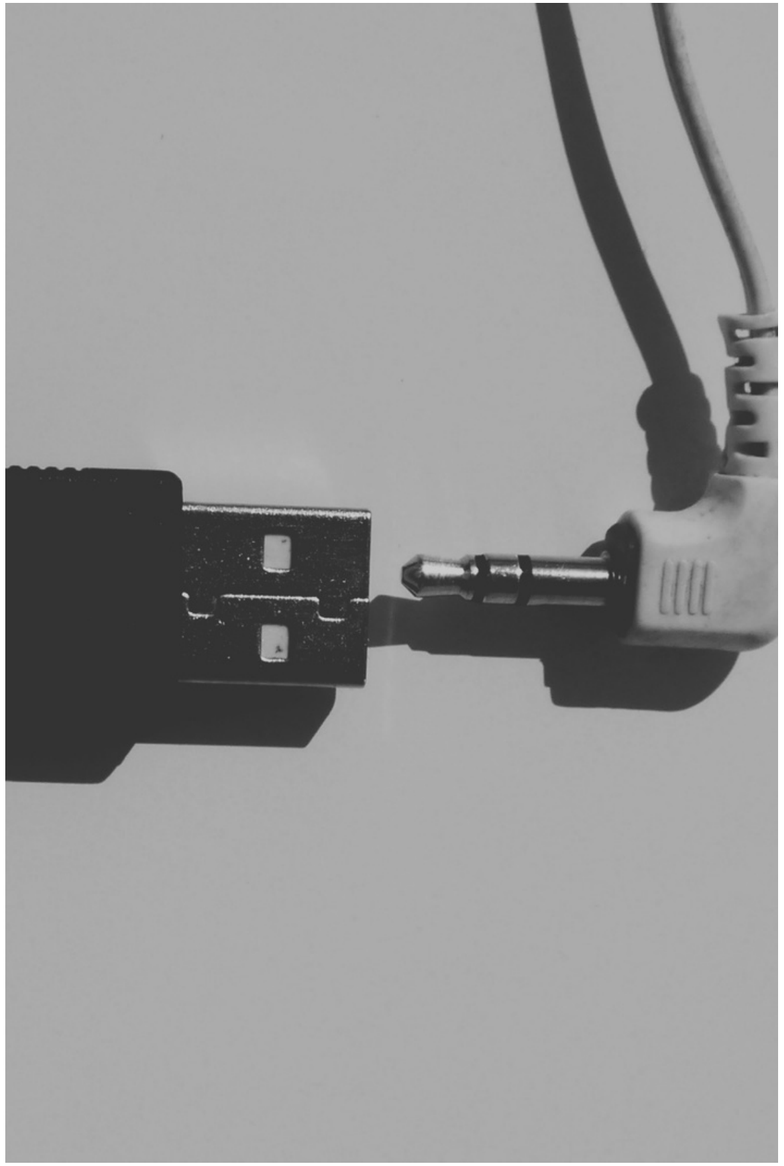
IN THE MODERN DAY

Logistical Threat: Incompatible Outcomes

When a sufficient security strategy cannot be realised due to incompatibilities with existing infrastructure, these threats can be magnified by policy and guidelines that aren't in tune with technology requirements.

Outcome

When security is treated as a strategic outcome seperate of other strategic goals it can create a sense of false choice, where every concession to the business is seen as a loss for security, and every security initiative is seen as a blow to business efficiency.



IN THE MODERN DAY

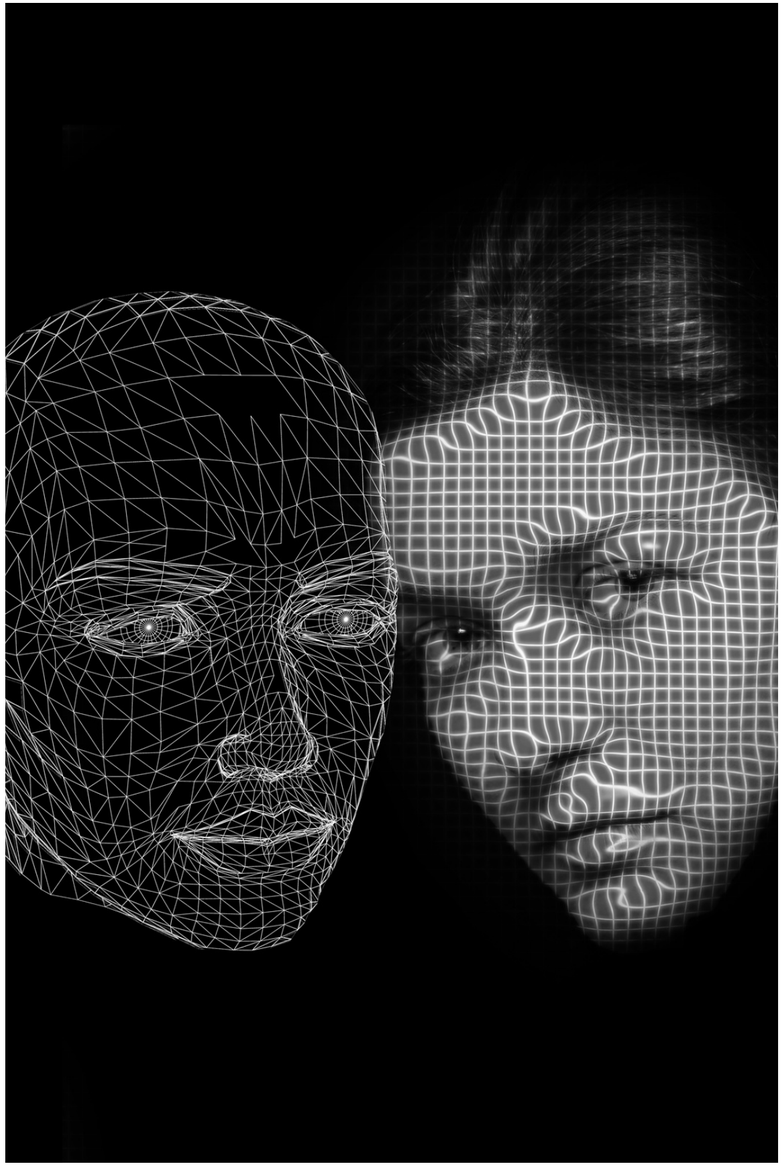
Emotional Threat: Fear & Doubt

When security leadership, or the security group rely on the fear uncertainty and doubt that is driven by the media to inform and define their security roadmap.

Outcome

When security decisions are informed by fear and doubt it can make unreasonable security decisions seem perfectly valid and justified. This can be made particularly bad when there are political, logistical and psychological threats also at play.

IN THE MODERN DAY



Psychological Threat: Unconscious Bias

The threat that comes with people being people, and having differences in how they process information, interact with technology, learn, gain new information and approach their own knowledge gaps.

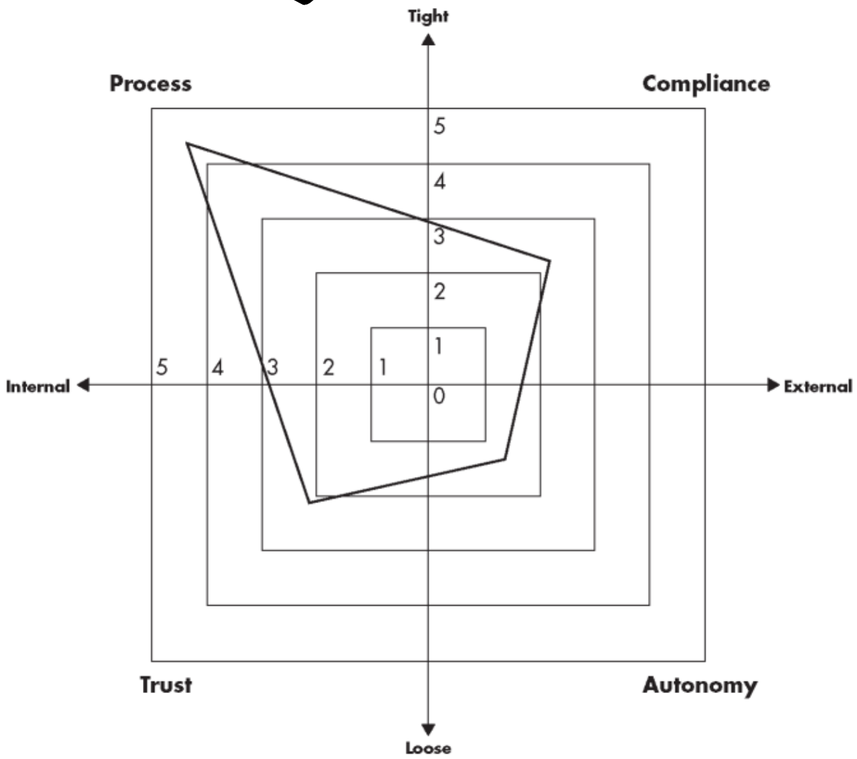
Outcome

Cultural differences can result in personality clashes that make solving problems difficult between employees. While the inaccessibility to information can make it difficult for people to participate in a meaningful way. Ego-based issues can result in logistical and technical threats.

SECURITY TOOL #3

Security Cultures Diagnostic Survey

- 10 questions, with four responses that align to the four quadrants of the the competing security cultures framework
- Response choices force the taker to differentiate between the relative importance of:
  - Stability and standardisation,
  - External validation and review,
  - Adaptability and freedom of choice, and
  - A sense of shared community and responsibility
- Maps directly onto the Competing Security Cultures Framework which defines 4 types of security cultures: process-based, compliance-based, trust-based and autonomy-based.



CASE STUDY #3

Summary

- Other cultural impacts can be observed in organisations:
  - Logistical threats impacting how people develop long term strategy, and handle immediate security concerns
  - Emotional threats defining how we assess security vulnerabilities, define our roadmaps, and meet objectives
  - Psychological threats subconsciously telling us how we handle everyday interactions, present information to people not deeply embedded in the industry, and how we handle the realisation we aren't omnipotent
- We can use the Security Cultures Diagnostic Survey to survey the organisation on how they perceive our day to day operations and where our subconscious and conscious priorities lie.

TYING IT ALL TOGETHER

COMPETING SECURITY CULTURES FRAMEWORK

- CSCF represents a “top-down” approach to understanding and changing your information security culture
- You can use the CSCF to orient yourself broadly in terms of your organisation's values and assumptions about security, and to identify areas of competition and potential cultural risk
- It's like a real-world map in that you can look at it and decide, “We're too far west. We need to go east”
- The CSCF does not tell an organisation exactly how to get where it wants to go

SECURITY FORCE BEHAVIOURAL MODEL

- The behaviours shown by the Security FORCE are designed to provide the more “bottom-up” perspective
- Understanding information security as both culture and behaviour is an important insight
- Highly reliable organisations are often too busy doing what they do, surviving and thriving, to worry about assigning labels like "high reliability” to themselves

SO, WHAT NEXT?

CHECK IN WITH YOURSELF →

Shaping organisational culture is a massive task that can't be done alone. Depending the state of the existing culture there could be a lot of work and there might even be pushback from your coworkers who value the status quo or managers who benefit from the existing power imbalances that may exist.

01

TALK TO YOUR COWORKERS →

Recognise your natural bias and challenge that by speaking to your coworkers, this feedback will also help you understand where things stand before you have the opportunity to measure and analyse which helps you build a case for the next step.

02

GET BUY IN →

Have security be such a part of organisational activity that people think about security even when making decisions that they haven't been specifically told are security related. And so you need to draw in leaders to make them understand the concerns at hand.

03

START TO MEASURE →

Learn to measure and analyse the security culture to a level where you know enough about it and how it works to make changes that will stick, and that you can demonstrate have stuck.

04

RESOURCES

ESSENTIAL CYBERSECURITY SCIENCE - JOSIAH DYKSTRA
ISBN: 978-1-491-92094-7

PEOPLE-CENTRIC SECURITY: TRANSFORMING YOUR ENTERPRISE SECURITY CULTURE - LANCE HAYDEN PHD
ISBN: 978-0-071-84679-0

COLLAPSE: HOW SOCIETIES CHOOSE TO FAIL OR SUCCEED - JARED DIAMOND
ISBN: 978-0-143-11700-1

SECURITY CHAOS ENGINEERING - AARON RINEHART, KELLY SHORTRIDGE
ISBN: 978-1-492-08034-3

APPLE'S CHILD PROTECTION FEATURES SPARK CONCERN WITHIN ITS OWN RANKS -SOURCES
HTTPS://REUT.RS/3KSVJXG

SLACK ROLLS BACK PARTS OF ITS NEW DM FEATURE OVER HARASSMENT CONCERNS
HTTPS://BIT.LY/3BHY1EG

```
IPTABLES -A OUTPUT -P TCP --DPORT 3389 -J DROP
IPTABLES -A INPUT -P TCP --DPORT 3389 -J DROP
```