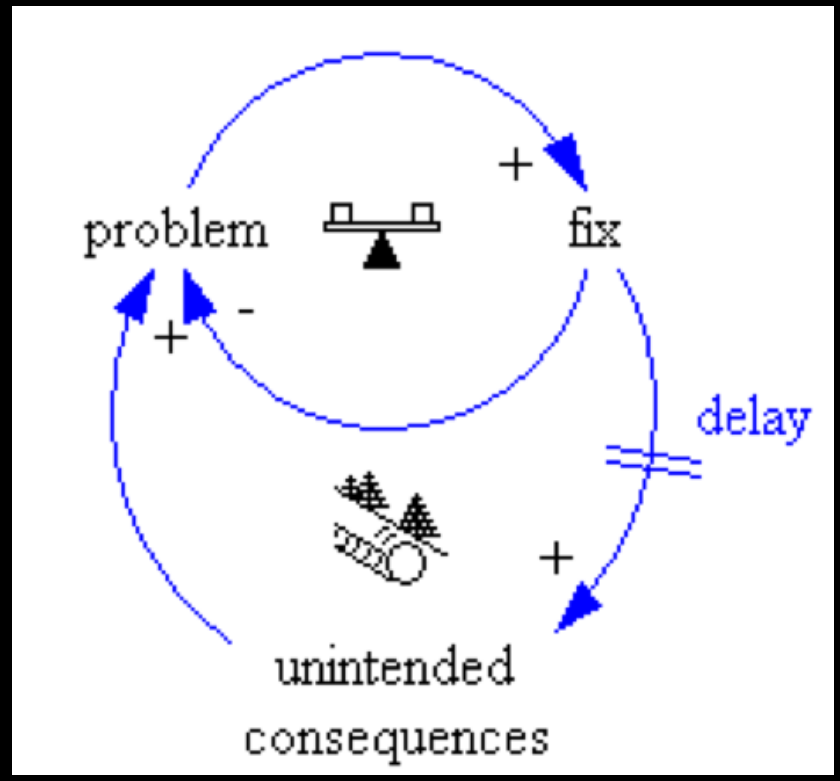
Build Secure Solutions Successfully with Systems Theory

PRESENTED BY:

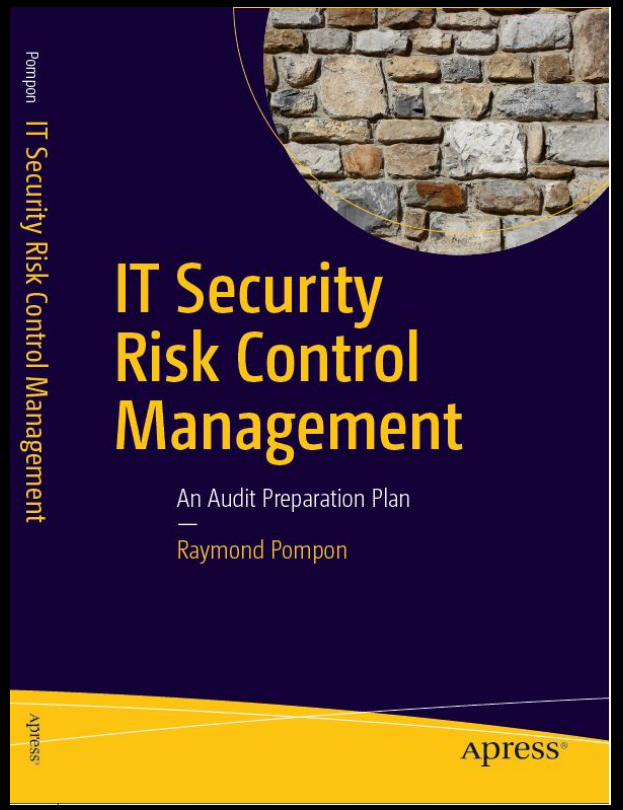
Ray Pompon, F5 Labs



Feb 2017

Ray Pompon

- F5 Labs - Principal Threat Researcher Evangelist
- Infragard, Sector Chief, IT and Finance
- Former head of InfoSec North America & Asia, global financial services company
- Author, *IT Security Risk Control Management: An Audit Preparation Plan*
- R.Pompon@f5.com
- @dunsany



Introduction

Security is “failing”

CNN tech

Yahoo says data stolen from 1 billion accounts

by Seth Fiegerman @sfiegerman

December 15, 2016: 4:30 AM ET

CNBC Search Quotes, News & Video

HOME

THE HACKING ECONOMY

Federal Government Confirms That It Still Sucks at Cyber Security

Arik Hesseldahl
Monday, 1 Feb 2016 | 12:31 PM ET

The Atlantic Sponsor Content: What's this? KPMG

Cyber Security: A Failure of Imagination by CEOs

Nearly a third of CEOs in KPMG's latest global survey identified cyber security as the issue having the biggest impact on their companies today—and only half (49 percent) say they are fully prepared for a cyber event.

NOV 29, 2016 @ 11:59 AM 2,979 VIEWS

Forbes

World's Biggest Mirai Botnet Is Being Rented Out For DDoS Attacks

Lee Mathews, CONTRIBUTOR

Observing, pondering, and writing about tech. Generally in that order

Opinions expressed by Forbes Contributors are their own.

ZDNet VIDEOS SMART CITY WINDOWS 10 CLOUD INNOVATION SECURITY DATA CENTERS MORE NEWSLETTERS ALL WRITERS

History repeating: How the IoT is failing to learn the security lessons of the past

The massive cyberattacks which took down some of the most popular websites on the internet show that device manufacturers are not learning from the mistakes of the past.

By Danny Palmer | October 25, 2016 -- 08:16 GMT (01:16 PDT) | Topic: Security

We have lots of security tools, yet…

CONSUMERAFFAIRS Consumer News Buyers Guides For Businesses

Just how effective is antivirus software?

IT security experts increasingly ask the same question

07/08/2016 | ConsumerAffairs | Internet

By Mark Huffman

Mark Huffman has been a consumer news reporter for ConsumerAffairs since 2004. He covers real estate, gas prices and the economy and has reported extensively on negative-option sales. He was previously an Associated Press reporter and editor in Washington, D.C., a correspondent for Westwoood One Radio Networks and Marketwatch. Read Full Bio→

REUTERS Companies look beyond firewalls in cyber battle with hackers

Companies look beyond firewalls in cyber battle with hackers

By **Tova Cohen** | TEL AVIV

With firewalls no longer seen as enough of a defense against security breaches, companies are looking at new tools to foil hackers trying to enter a computer network.

Death of the enterprise VPN - if remote access is not secure what comes next?

The Target hack of 2014 was a warning that VPNs are now a liability

John E Dunn
April 27, 2016

VPNs are the backbone of enterprise remote access and yet their security limitations are starting to pile up. The problem is that the very thing that once made them so useful, network access, is now their biggest weakness. As the 2014 attacks on retailers Target and Home Depot painfully illustrate,

GOVINFO SECURITY®

Why Training Doesn't Mitigate Phishing

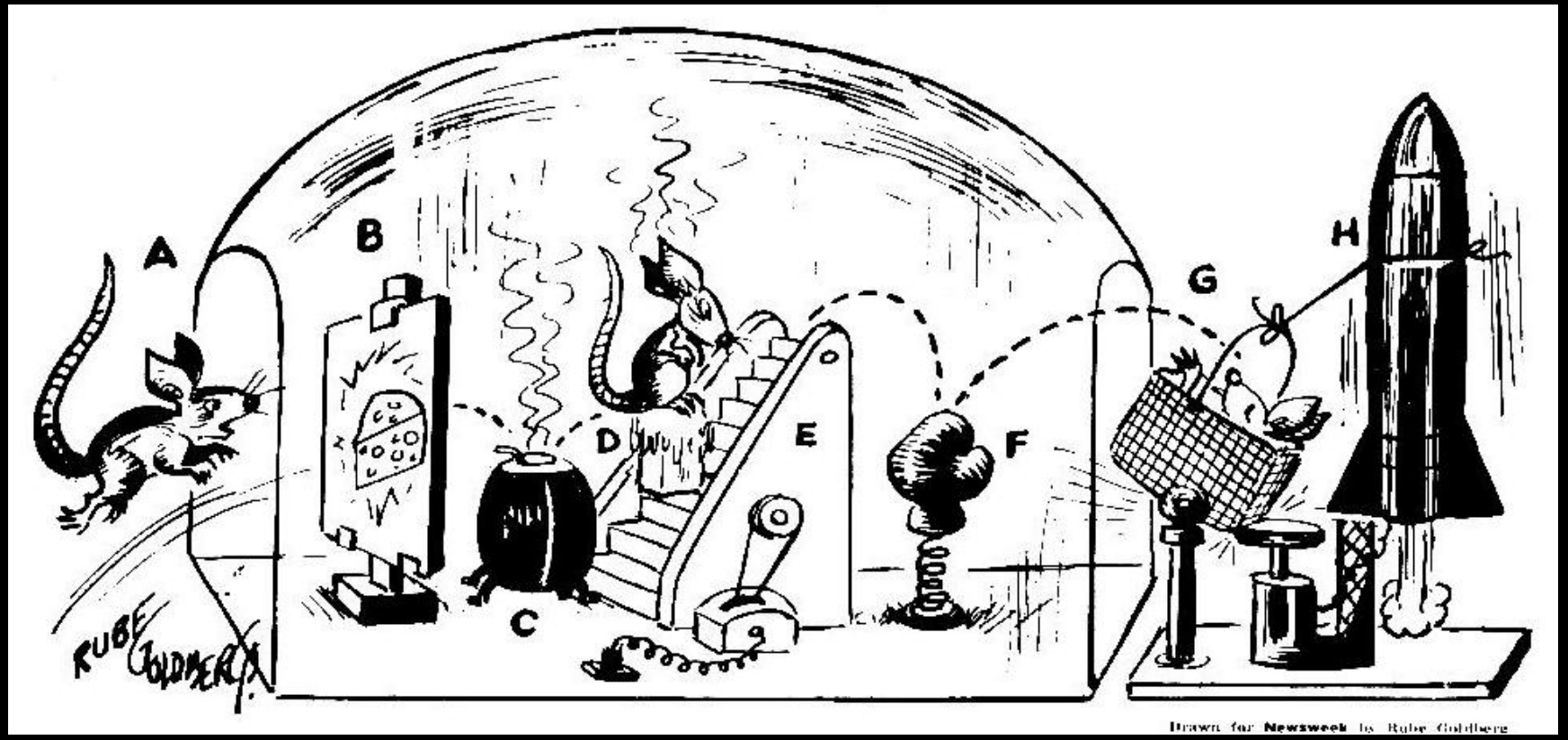
Study Finds Embedded Training Is Ineffective

Eric Chabrow (GovInfoSecurity) · January 7, 2014 · 10 Minutes · 4 Comments

They don’t work as well in our environments as we thought

Poor assumptions, simplistic approaches

- “I know the system well, so if I make a **little** change, then I know what will happen…”



Most IT infras are Rube Golberg machines – how can you make a “little” change w/o consequences?

The complex systems trap

- Our organizations are a complex system with legal, technical, business, social, financial subsystems
- Many of the variables and sub-systems are connected by feedback relationships.
- Small events that are separated by distance and time can be the cause of significant changes in complex systems
- The mode of failure of a complex system cannot ordinarily be predicted from its structure
- Security is frequently an *emergent* property of a system

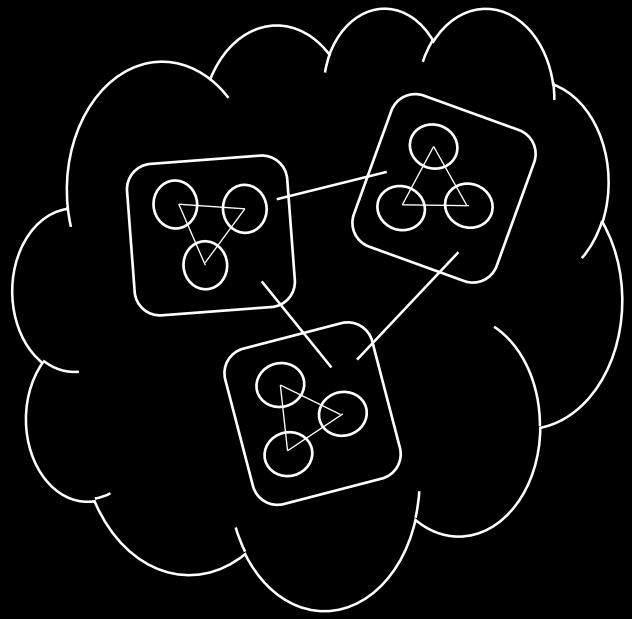
We cannot treat complex systems as simple

- IT Infra are piecemeal designs,
  a patchwork of multiple point solutions
- Security controls are “added on”
- Organizations are in constant motion
- Users are treated as passive objects
- Best practices trap – “This worked once upon a time for these folks,
  therefore it should work for you, now.”

Systems Theory

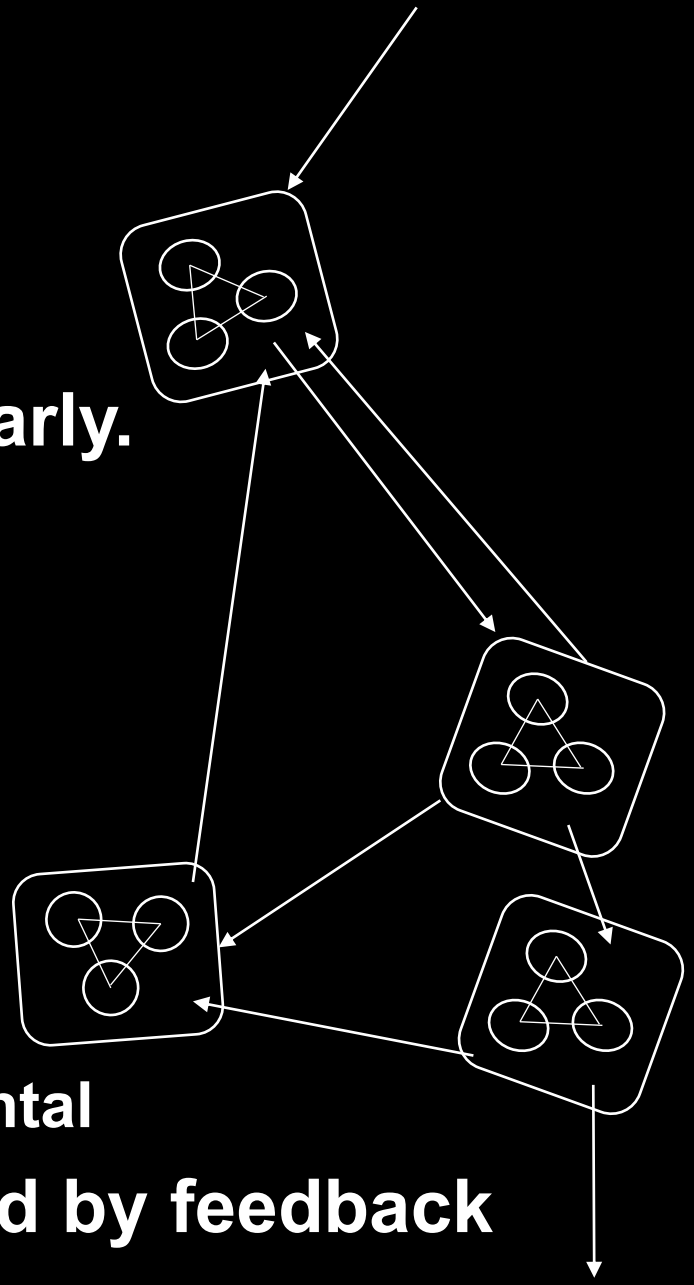
Intro to Systems Theory

- Holistic way of thinking
- Reduces complexity by modelling it
- Acknowledges & incorporates “invisible” factors
- Views problems as “unintended consequences”
- Looks at how things change and why
- Cause & Effect are Cyclical not Linear
- Tracks feedback loops and adjusts them



How to think about a System

- The whole is greater than the sum of the parts
- Large number of elements interacting non-linearly.
  A minor change could produce major consequences,
  therefore everything has trade-offs
- Everything is connected –
  elements constrain and compel each other
- Systems have context and history:
  The past is integrated into the present
- Systems have many levels or facets:
  legal, technical, business, social, financial, environmental
- Systems maintain equilibrium and are governed by feedback

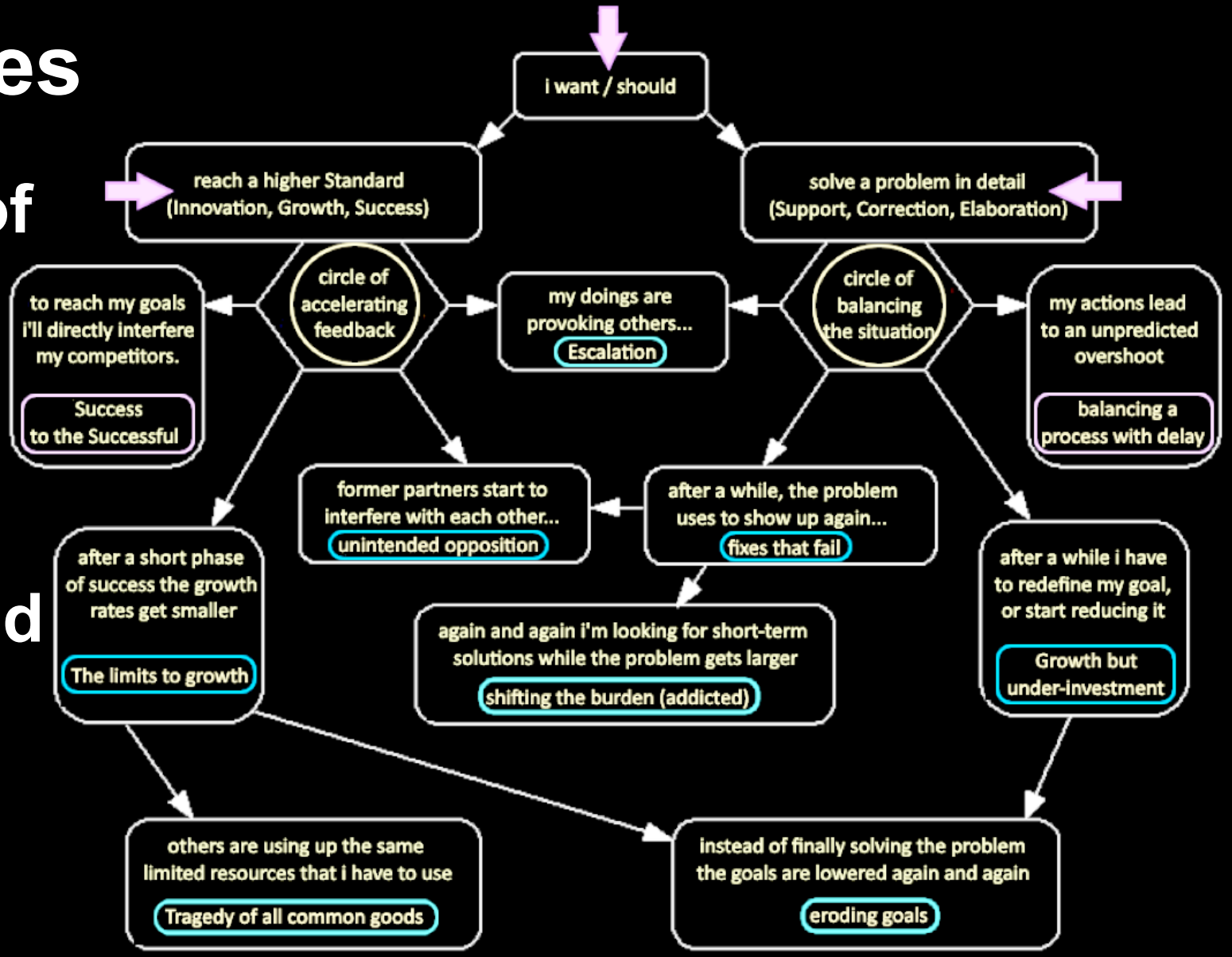


Altering a system's behavior

- **Adjust parameter for rate of change**
- Bug bounties, Deployment process, Rollout of controls
- **Alter the rules**
- Security policy, approval process, ownership of assets/risk
- **Adjust buffers & flows**
- Budget, workload, personnel
- **Regulate feedback loops (positive, negative, delays)**
- Audits (internal/external), awareness rewards
- **Alter information flows**
- make things visible/invisible (risk, cost, compliance)
- **(Re)define the goals/ paradigm**
- Acceptable risk, culture, leadership

System Archetypes

- Describe patterns of behavior in organizations
- Models to help frame thinking
- Uncover unexpected dependencies and reactions

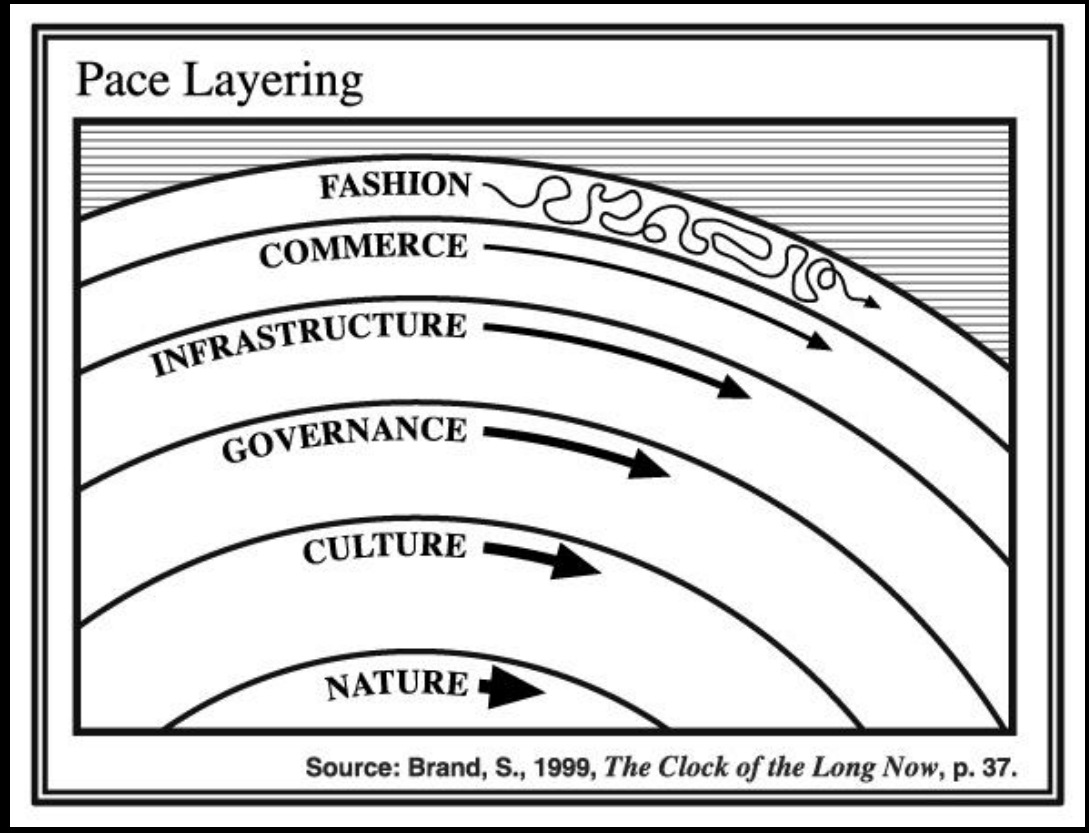


https://en.wikipedia.org/wiki/System_archetype

Pace Layers

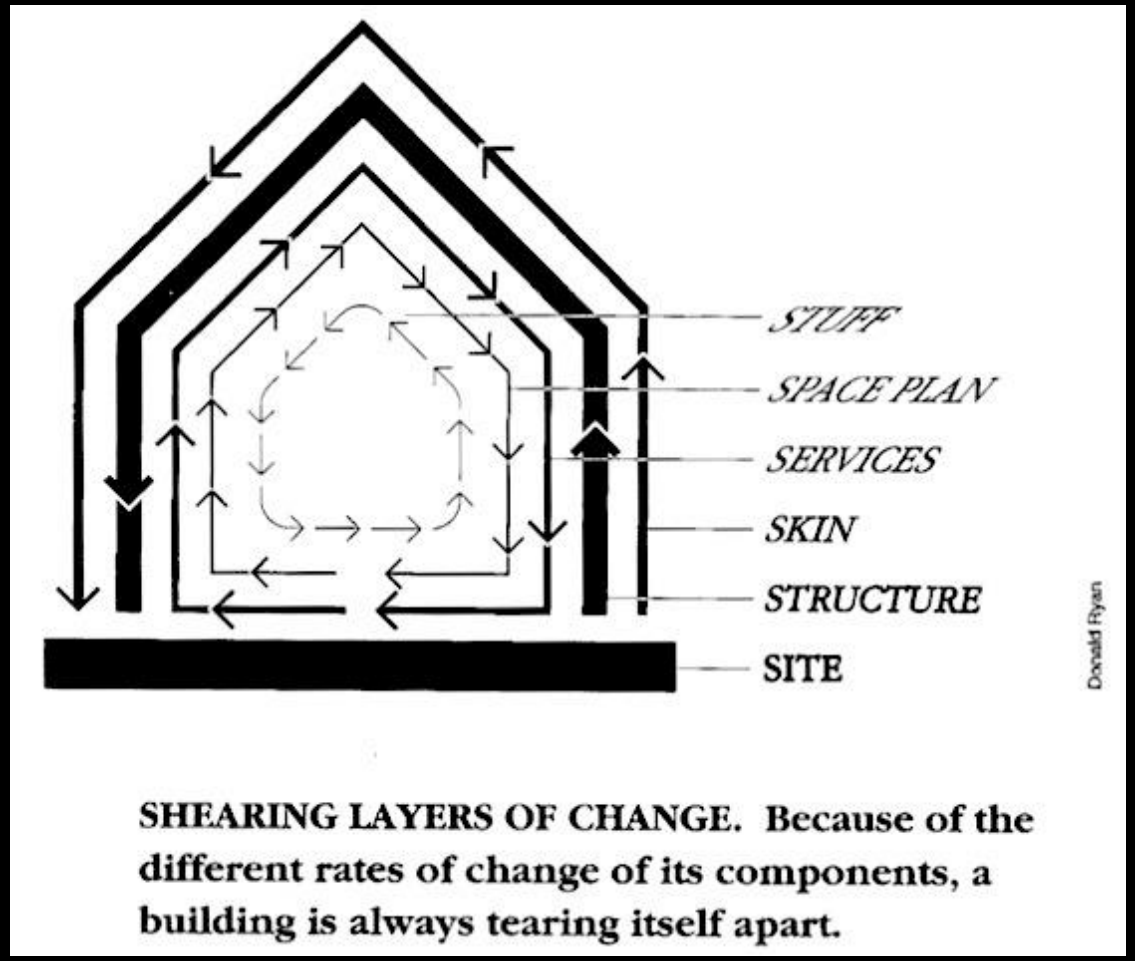
New archetype: Pace layers

- From Stewart Brand's How Buildings Learn
- Began w/ physical architecture
- Treat organization organically
- Different layers age differently



Pace Layer Behavior

- Faster layers provide innovation & originality
- Slower layers learn and/or remember
- Slower layers are viscous, move in spurts
- Differing rates of change, creates friction/shear
- Moving beyond pace is a “revolution” - turbulence

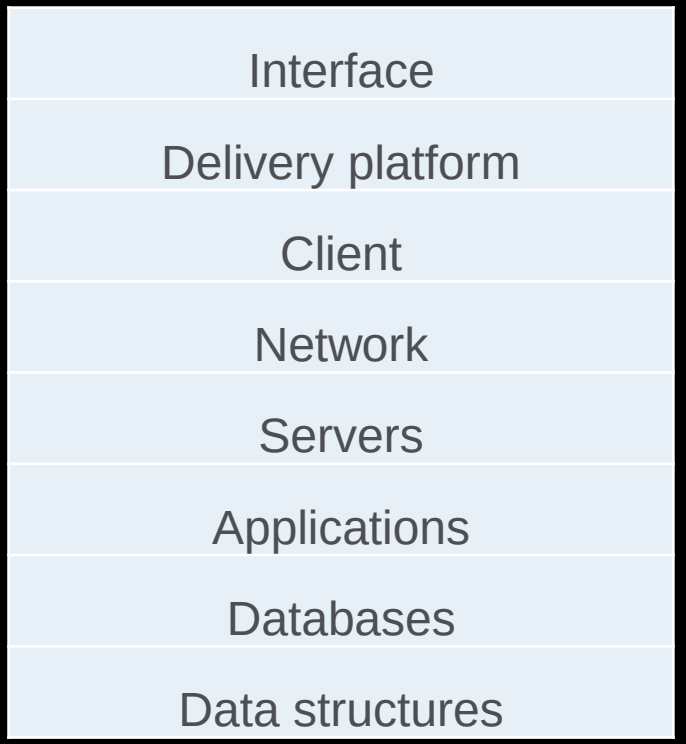


Brand, Stewart, C.(1994). How Buildings Learn: What Happens After They’re Built, Viking Press

Pace Layers in the IT world

IT Security considerations:

- Data flows down and accretes at bottom
- The Internet is a copy machine
  – Kevin Kelly
- Data leaks along the way
  – Norton's law



Kevin Kelly - "If something can be copied and it touches the Internet, it will be copied."
https://twitter.com/kevin2kelly/status/7243270678656122 89

Norton's law - "Over time, all data approaches deleted, or public"
https://medium.com/message/hello-future-pastebin-readers-39d9b4eb935f#.ulcq6lrmu

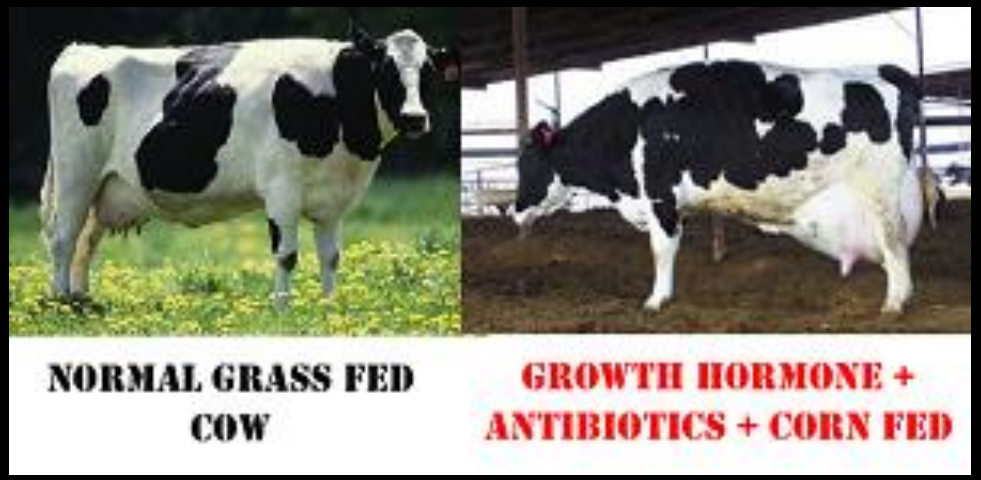
Pace layers to help model security scenarios

- What layers aren't covered by controls?
- Access control at each layer boundary?
- Can you map threats through the layers?
- Can you reduce shear by decoupling layers?
- Solve problems at the right layer:
  I.e. uptime problem: Change control to stabilize vs adding more high-avail tech

Shifting the Burden

System Archetype: Shifting the burden

- The solution to a systemic problem disguises the symptoms but does not solve the underlying problem
- Shifting problems to another part often go undetected because they appear "solved”
- We get dependent on this “solution”

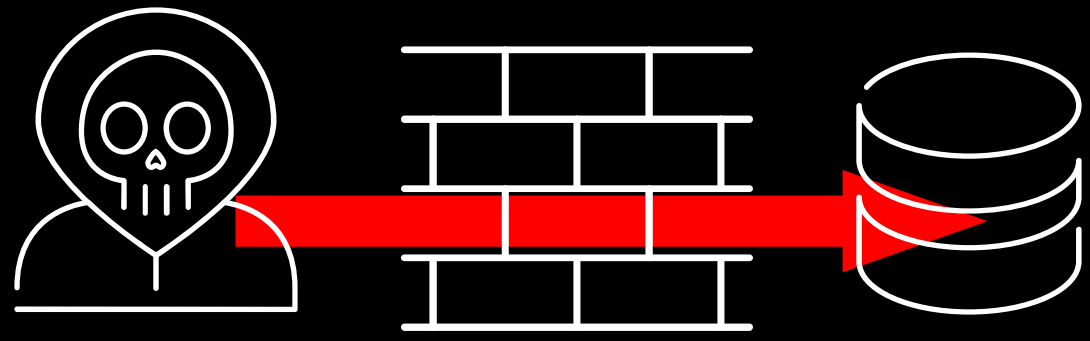


Shifting the burden - Firewalls

- Firewalls originally built to filter access to network services and applications with weak security

- Now firewalls are considered “essential”
- Internal networks bigger and weaker than ever
- Penetrate & Pivot – Crunchy shell, chewy center

- Fixing the weak services & apps?

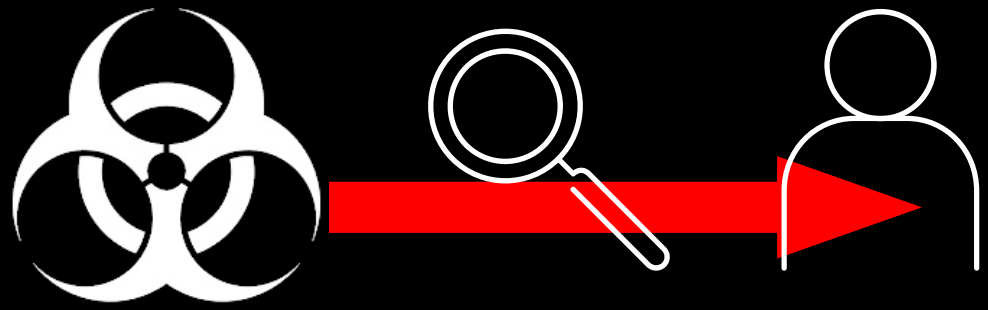


Shifting the burden – Anti-virus

- Originally built to remove infections taking advantage of weak OS and app software

- Now antivirus is considered “essential”
- Anti-virus bigger and more complex than ever
- Arms race between AV and malware writers

- Fixing the weak OS and app software?



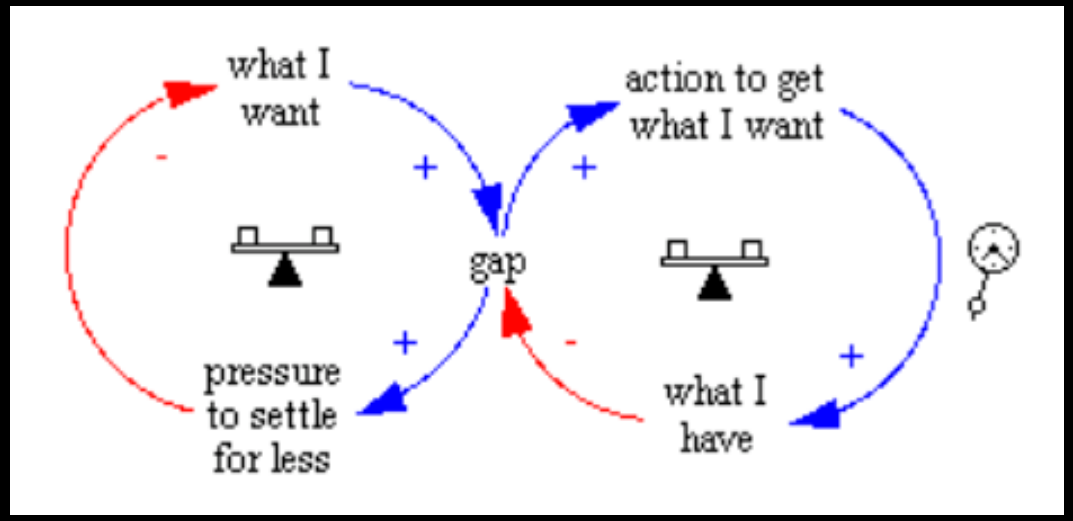
Shifting the burden - solutions

- Who is actually paying to compensate for holes?
- How can you make risk “visible” at the right place?
- How can you shift the burden to those who have the most control over it?
- How much leverage should security have in System Acquisition, Development, and Maintenance?

Drifting Goals

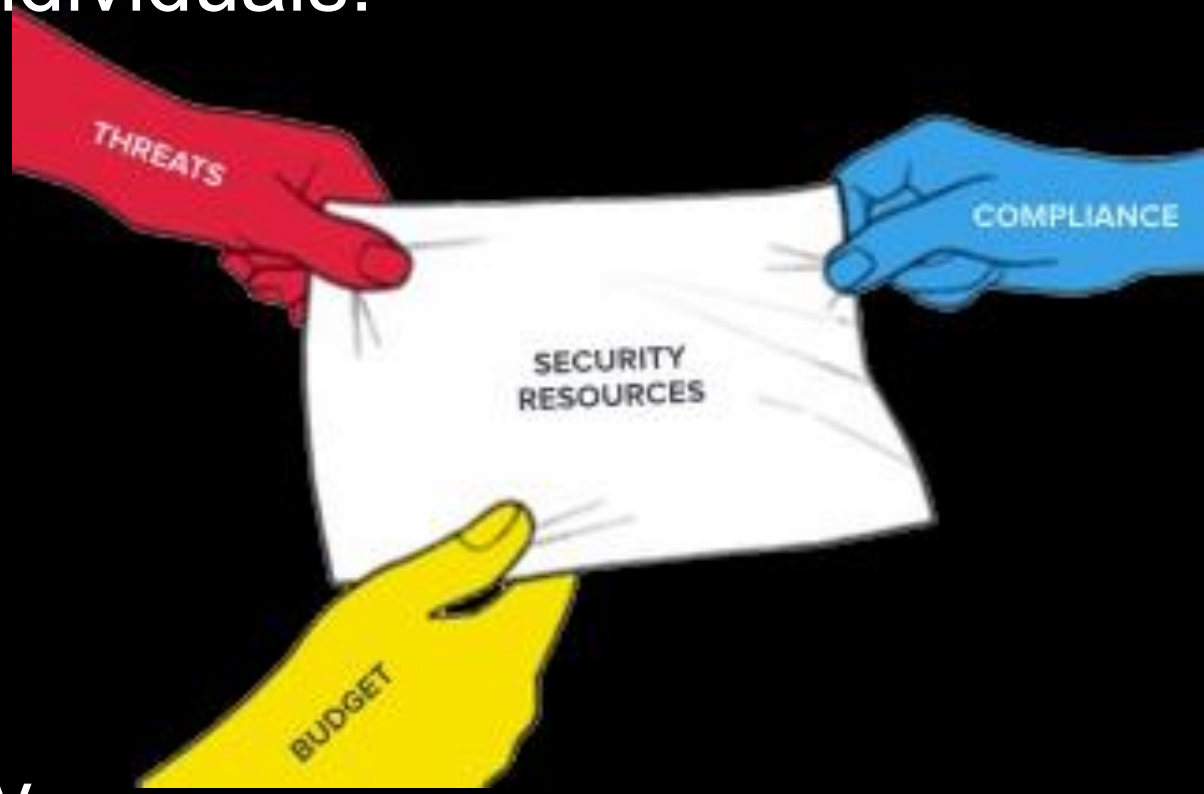
System Archetype: Drifting goals

- A drifting goals structure is composed of two balancing loops which interact in such a way that the activity of one loop actually undermines the intended balance the other loop seeks to achieve.
- Lowering your standards to achieve a “win”



Drifting goals: The Compliance System

- The bigger the system, the narrower and more specialized the interface with individuals.
- Systems once created, are hard to get rid of
- Systems expand and encroach over time
- As systems grow complex, they tend to oppose their stated function.



Drifting goals - solutions

- Disconnect compliance feedback loop from security goals
- Security primary, compliance secondary
- Treat risk and compliance are both separate requirements
- Understand the gap between compliance & security, mitigate what’s fallen in the gap

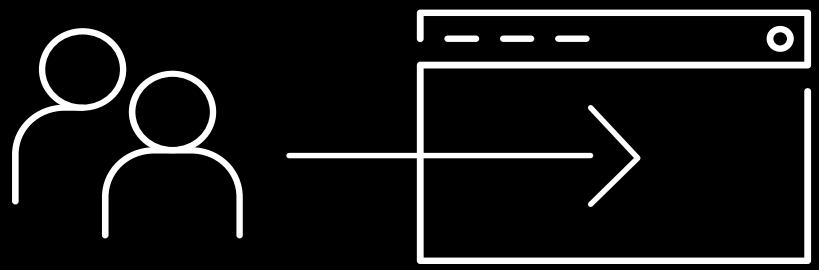
Fixes that fail

System Archetype: Fixes that fail

- Solution is rapidly implemented to address an urgent problem
- The problem appears to be solved but really only masking symptoms
- Side effects and unintended consequences appear later, that undo the solution

Fixes that fail: Overly Restrictive Controls

- Just “encrypt everything”
- Users not allowed to copy files, run programs
- Absurdly difficult access controls
  12 char passwords, rotate monthly



- Can result in even more breaches as users attempt to work around restrictions.

Fixes that fail - Solutions

- You can’t sprinkle security fairy dust onto a running system to secure it – you have to redesign it

- Bounded rationality, people need to get things done
  https://en.wikipedia.org/wiki/Bounded_rationality

- Fixing a running system - Isolate and fix
  Isolate important stuff from the unstable systems, modifications only thru a controlled process
  http://www.itpi.org/the-visible-ops-book-series.html

Conclusion

System’s theory lessons for security

- When working in security, consider the whole picture
- Different parts of a system “breathe” in different rates
- Security is not an add-on, it’s an intrinsic quality
- Look for side effects, keep your eye on the goal
- Start small, test, iterate, expand

Systems theory reading

- Thinking in Systems: A Primer
  - Donnella Meadows

- An Introduction to General Systems Thinking
  - Gerald Weinberg

- The Fifth Discipline: The Art and Practice of the Learning Organization - Peter Senge

"People are more comfortable with old problems than they are with new solutions."
- John Maxwell