PCI Security Standards Council

Learning From Safety-critical Industries

Control Failure Is Normal, Deal With It.

PCI Security Standards Council

John Elliott

Consultant

PCI ROCKS

Were You at the Community Meeting When?

John Nance
2015

Jeff Skiles
2017 & 2018

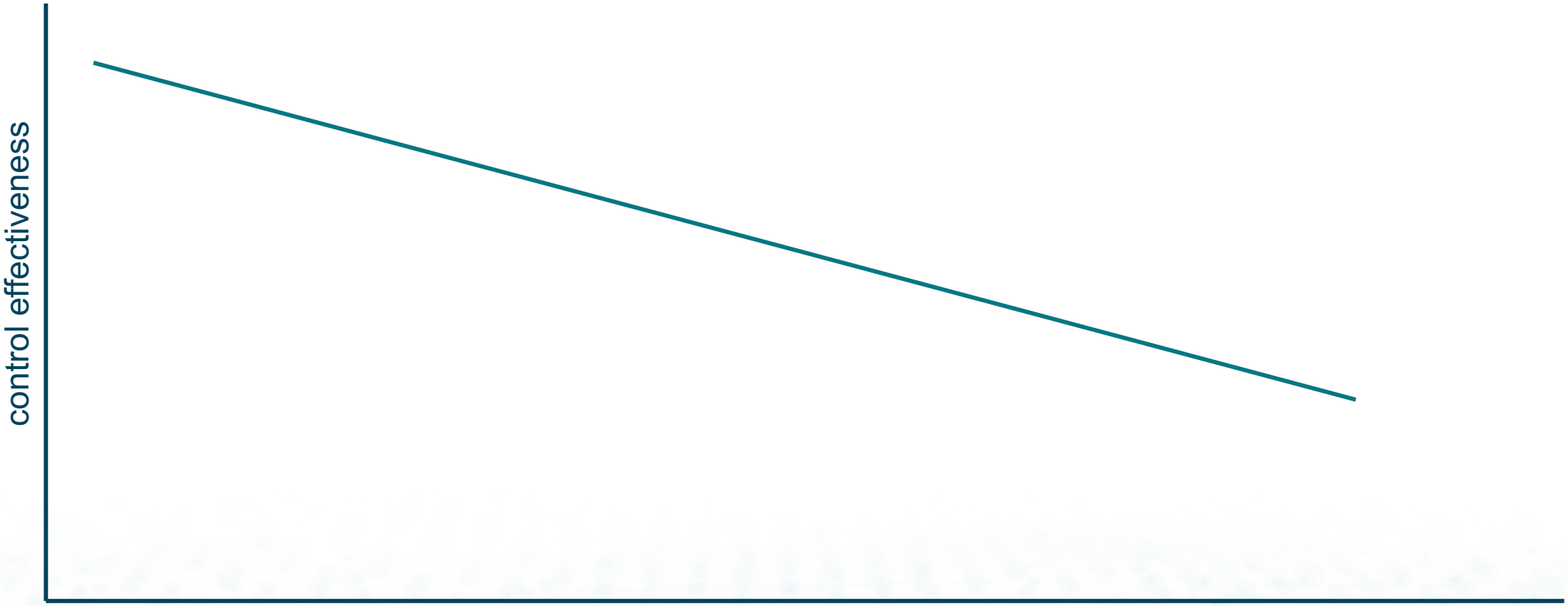
PCI Security Standards Council®

My Own Aviation Experience

PCI Security Standards Council®

Why PCI DSS Has Annual Assessments

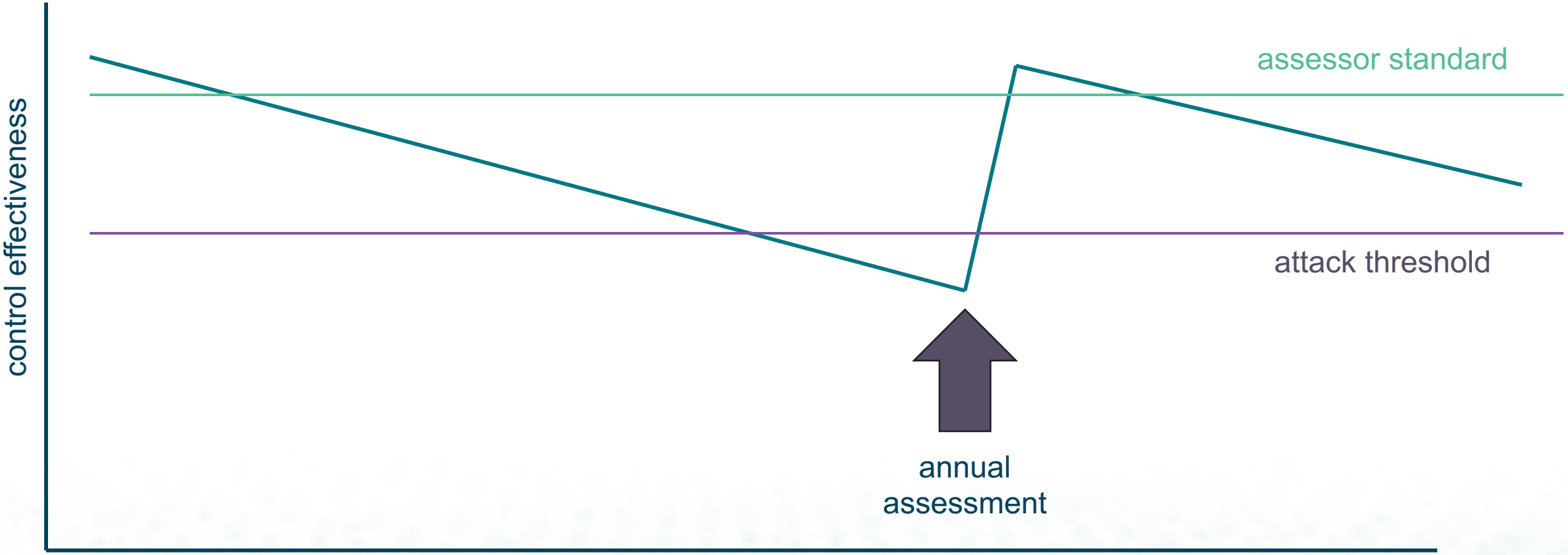
(This is what I used to say)



PCI Security Standards Council

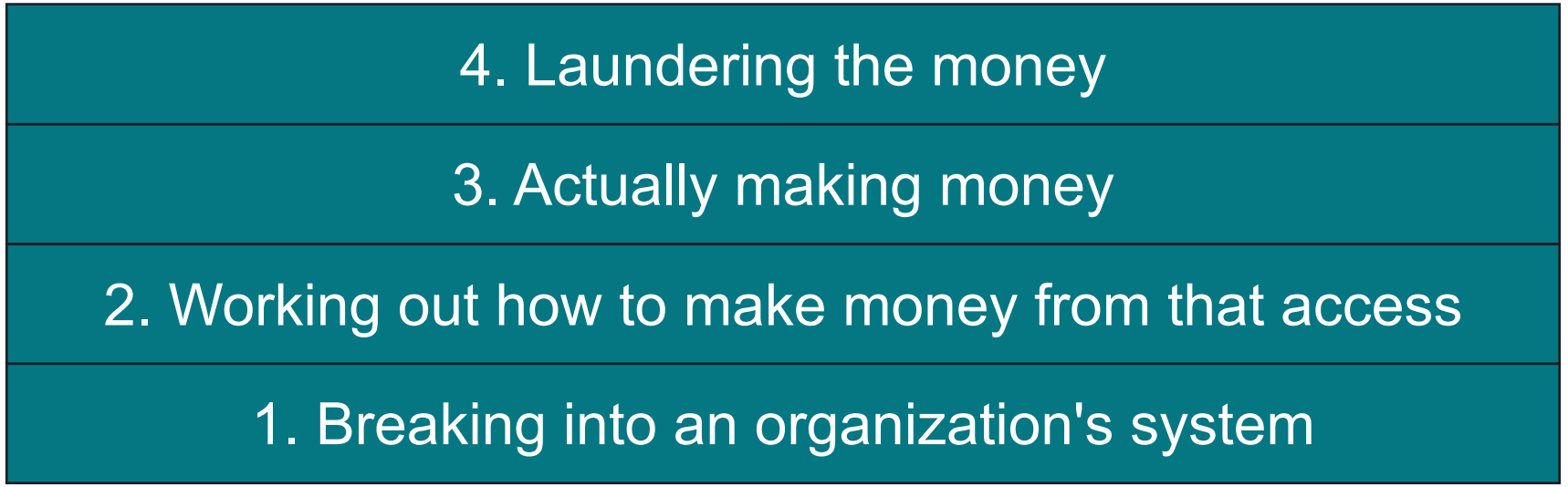
Why PCI DSS Has Annual Assessments

(This is what I used to say)



PCI Security Standards Council

Vertical Disintegration



Vertical Disintegration

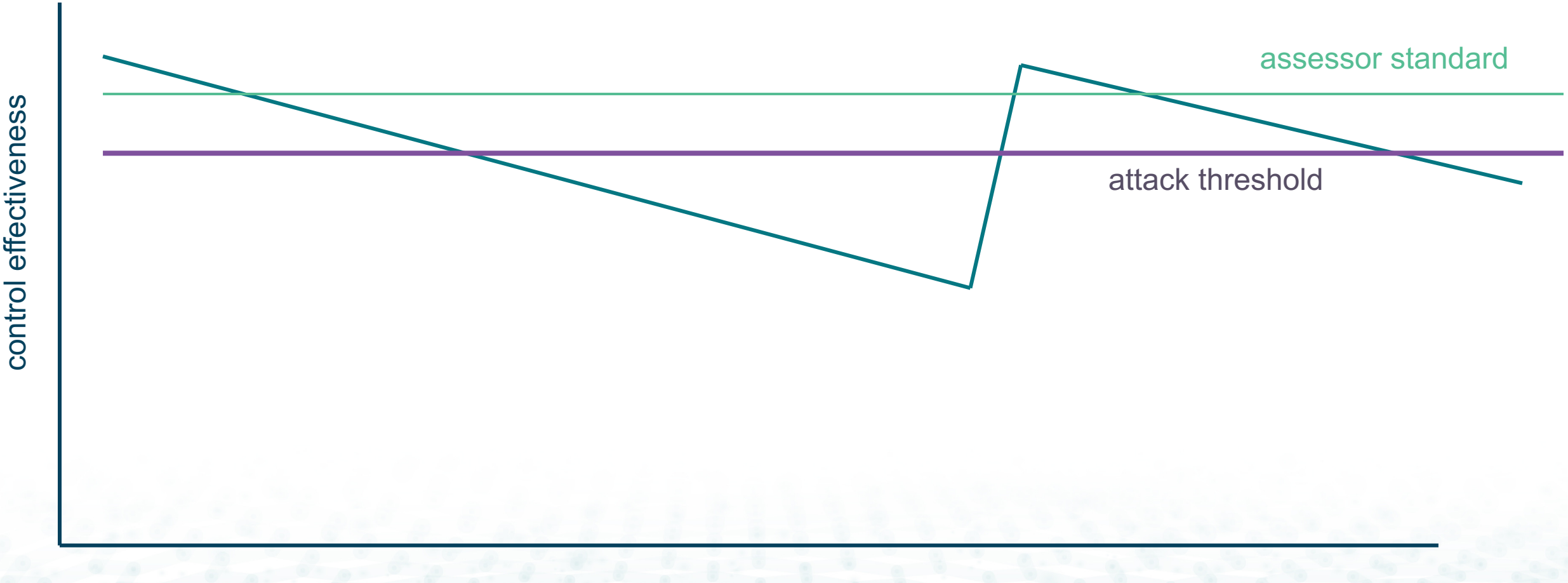
4. Laundering the money

3. Actually making money

2. Working out how to make money from that access

1. Breaking into an organization's system

Why PCI DSS Has Annual Assessments



PCI Security Standards Council

“The firewall was incorrectly configured.”

Forensic Investigator

PCI Security Standards Council®

“The server that was attacked was not patched.”

Forensic Investigator

PCI Security Standards Council®

“We took advantage of a misconfiguration.”

Penetration Tester

PCI Security Standards Council®

“Not all systems were running the application sandbox.”

Penetration Tester

PCI Security Standards Council®

“We knew that one server wasn’t patched.”

Internal Information Security

PCI Security Standards Council®

“That was scheduled to be fixed next week.”

Internal Information Security

PCI Security Standards Council®

“Dave was just looking at that …”

Dave’s manager

PCI Security Standards Council®

Why Do Controls Fail?

Natural Entropy

- Never fully implemented
- Sometimes software does not do what you expect
- Misconfiguration
- Not updated
- Removed “temporarily” because something stopped working
- The person who understood them left

Why Are Controls Totally Missing?

Change

- Never fully implemented across all devices
- Removed by users
- New systems added to scope
- Removed “temporarily” because something stopped working
- Didn’t re-license

Aviation doesn’t “do safety”

Aviation is safe

PCI Security Standards Council®

Key Concept

Humans are fallible

Key Principles in Safety-Critical Industires

Engineer fallibility out

Compensate for fallibility

Reduce fallibility

Learn from errors and incidents

Engineer fallibility out

How can we make it so that a human error doesn't affect anything?

- Electronic toolboxes
- Stall control

Engineer fallibility out

How can we make it so that a human error doesn't affect anything?

- Software auto-update
- Multi-factor authentication
- Software signing
- Anti-malware

(we used to say don't click on files)

Compensate for fallibility

How can we catch human errors before they have an effect?

1. In business-as-usual operations
2. In rare events
3. Continual assurance checks to catch issues before they have an effect

Compensate for fallibility

●○○

How can we catch human errors before they have an effect?

1. In business-as-usual operations

- Checklists
- Doors to automatic and **cross-check**
- Steering bypass pin removed

After Push Back

PCI Security Standards Council®

Compensate for fallibility

●○○

How can we catch human errors before they have an effect?

1. In business-as-usual operations

- Checklists
- Dual-control

PCI Security Standards Council

Compensate for fallibility

●●○

How can we catch human errors before they have an effect?

2. In rare events

- Checklists
- Rehearsed plans

Compensate for fallibility

●●○

How can we catch human errors before they have an effect?

2. In rare events

- Incident response plan
- Rehearsed / tested

PCI Security Standards Council

Compensate for fallibility

●●●

How can we catch human errors before they have an effect?

3. Continual assurance checks to catch issues before they have an effect

- Prioritized checks

Compensate for fallibility

How can we catch human errors before they have an effect?

3. Continual assurance checks to catch issues before they have an effect

- Prioritized control tests

Compensate for fallibility

Requirement	Detail
1.2.7	**Six monthly** review of NSC configurations
3.2.1	**Quarterly** verification that there is no cardholder data present beyond specified retention period
7.2.4	**Six monthly** review of all user accounts and related access*
7.2.5.1	**Periodic** (based on TRA) review of access of system and application accounts *
9.4.1.2	Annual validation of security of offline media backup
9.4.5.1	Annual validation of inventory of physical media containing cardholder data.
11.2.1	**Quarterly** scanning for rogue wireless access points. (Optional, other non-scan technology may be used to meet the requirement)
11.3.1	**Quarterly** internal vulnerability scans
11.3.2	**Quarterly** external vulnerability (ASV) scans
11.4.2 11.4.4	Annual internal penetration test
11.4.3 11.4.4	Annual external penetration test
11.4.5	**Six monthly** CDE segmentation penetration test
12.2.2	Annual review of information security policy
12.3.1	Annual review of all TRAs every 12 months
12.3.3	Annual review of cryptographic inventory *
12.3.4	Annual review of hardware and software technologies
12.4.2	**Quarterly** assurance reviews of requirement 10.4 – daily log reviews
12.4.2	**Quarterly** assurance reviews of requirement 1.2.7 – config reviews of NSCs
12.4.2	**Quarterly** assurance reviews of requirement 2.2.1 – applying config standards to new systems
12.4.2	**Quarterly** assurance reviews of requirement
12.4.2	**Quarterly** assurance reviews of requirement 6.5.1 – Change management procedures
12.5.2	Annual (Six-monthly*) documentation and confirmation of scope
12.6.2	Annual review of security awareness program
12.8.4	Annual review of TPSPs compliance status
12.10.2	Annual test of incident response plan
12.10.2	Annual review of incident response plan

PCI Security Standards Council

1.2.2 | Change management of NSCs			
Days since last assurance check	Non-conformances found	Non-conformances still outstanding	Days to next assurance check
100	5	3	-10 Overdue
1.2.3 | Validity of network diagram			
Days since last assurance check	Non-conformances found	Non-conformances still outstanding	Days to next assurance check
100	1	0	80

No	Detail	Frequency (months)
2.2.1	Update of configuration standards and use of config standards for new builds	3
3.2.1	No cardholder data present beyond specified retention period	3
3.7	Where key custodians are used, all key custodians are still working for the entity and can produce their physical or digital key material (suggest every 4 or 6 months)	3
4.2.1.1	Validation of inventory of keys and certificates*	6
5.2.3	Review of systems where anti-malware solutions are not deployed based on period defined by TRA	6
5.3	Coverage of updated, functioning, anti-malware solution over the intended estate	2
5.4.1	Operation of automated anti-phishing mechanisms*	6
6.2.2	Annual secure software development training for developers	6
6.2.3	Code reviews	4
6.3.1	Identification of new security vulnerabilities and associated management	4
6.3.2	Validation of inventory of custom and bespoke software *	4
6.3.3	Critical- or high-vulnerabilities are patched within 30 days	3
6.4.3	Validation of inventory of JavaScript and associated authorization and justification of necessity.	2
6.5.1	Validation that change control procedures are being followed and correctly documented	3
7.2.3	Changes in user privileges are approved by authorized personnel	6

Reduce fallibility

How can we improve human performance?

- Mandatory training
- Peer-evaluation
- Fatigue management

Reduce fallibility

How can we improve human performance?

- Mandatory training
  - All users (as in 12.6.3)
  - All IT people
  - All information security people
- Purple-team exercises (trains the blue team)
- Manage stress and burn-out

  (especially in the SOC)

Learn from errors and incidents

How can we *engineer* or *compensate or reduce* to make sure this doesn't happen again?

- Formal post-incident review
- Contributory factor analysis
- Requires a *Just Culture*

Learn from errors and incidents

How can we *engineer* or *compensate or reduce* to make sure this doesn't happen again?

- Formal post-incident review
- Contributory factor analysis
- Requires a *Just Culture*

10.7.3 – Causes of control failure
12.10.6 – IRP modified according to lessons learned

PCI Security Standards Council

Establishing a Just Culture

Learn from errors and incidents

https://www.youtube.com/watch?v=kd4Bi36LI3E

PCI Security Standards Council

How do we change from “doing cybersecurity” to being cybersecure?

PCI Security Standards Council®

Summary

Lessons from safety-critical industries

1. Engineer fallibility out
   How can we make it so that a human error doesn't affect anything?
2. Compensate for fallibility
   How can we catch human errors before they have an effect?
   - In business-as-usual operations
   - In rare events
   - Continual assurance checks to catch issues before they have an effect
3. Reduce fallibility
   How can we improve human performance?
4. Learn from errors and incidents
   How can we *engineer* or *compensate* or *reduce* to make sure this doesn't happen again?

PCI Security Standards Council