OWASP
Open Web Application
Security Project

CISO 90 Day Plan

Nelson Chen, M.SC. IT

CISSP, CISA, CISM

Agenda

- Why are we here?
- Days 0 – 30
- Days 31 – 60
- Days 61 – 90
- Days 90+
- Infinity & Beyond

Avoiding Really Bad News!

Don’t be the Blocker!

Don’t be the Prophet of Doom

Toughest Part of the Job

CISO Post-Breach

Establishing Relationships & Trust

0 - 30

Selling CISO as a Service

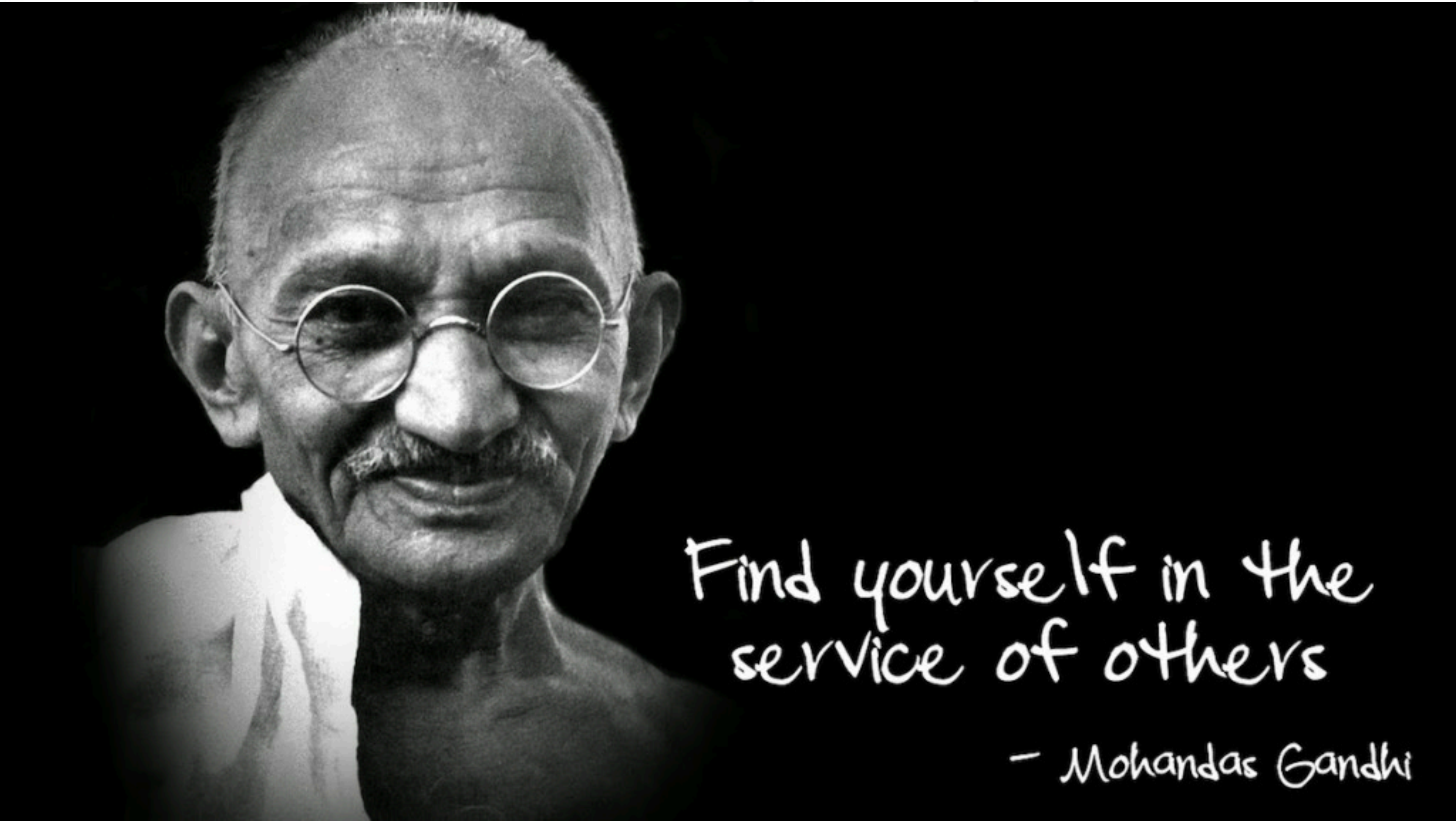
- Business enablement
- FUD is not the only pitch
- Education
- Shared responsibility
- Get support and buy-in
- Add Value!

Taking Initial Inventory

- Organizational Structure - Who’s who
  - Execs, BU Leaders, IT Ops, Internal Audit
- Existing Policies, Processes, etc.
- Existing Technologies
- Where’s the Data?
- Historical Security Incidents
- Shadow IT

Leading Towards Better Security

Servant Leadership



Find yourself in the service of others

– Mohandas Gandhi

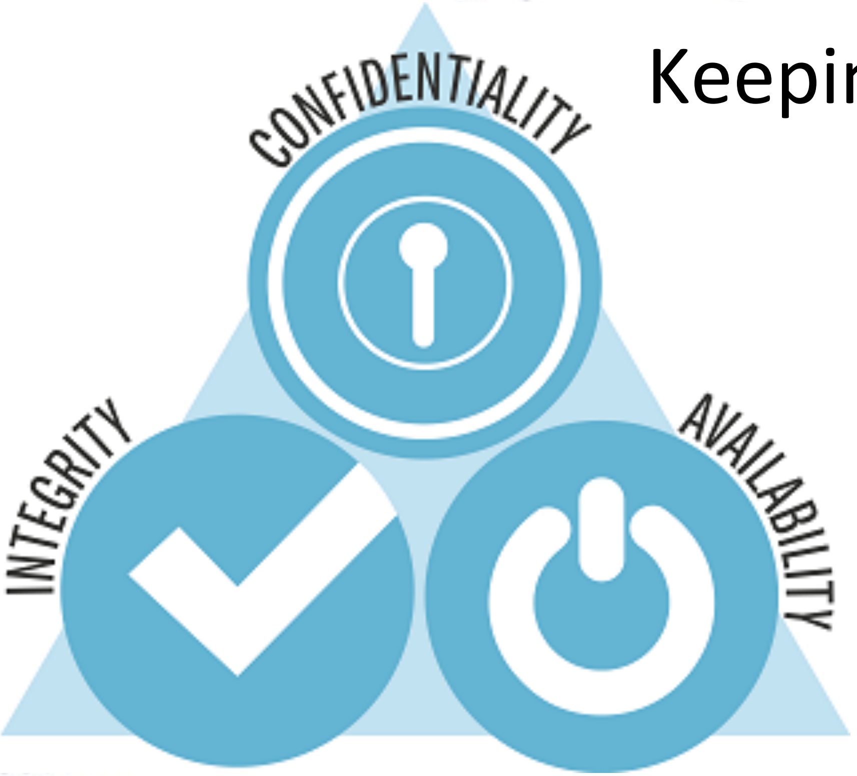
Security Surrounds us, Penetrates us and Binds us Together

LUCASFILM Ltd

Prioritizing & Project Kickoff

31 - 60

Back to Basics - CIA Triad



Keeping it secret

Keeping it together

Keeping it up

[Central Oregon Community College](#)

Fox-in or Fox-out?

Meet the new head of security.

Team or Committee?

Security Team Building

- BU InfoSec Officers – Legal, Finance, Sales, Marketing, HR, Development, IT, etc
- Committee driven
- Executive sponsor
- Internal audit is your friend
- Where are all the resources?

KissPNG

Security Committee Goals

- Business Security Mission Statement
- Aligning security with each BU
  - what are we protecting?
- Taking detailed inventory
  - Processes, Systems, Data, People
- Budgetize, Prioritize, Projectize
- Reporting directly to C-levels

KissPNG

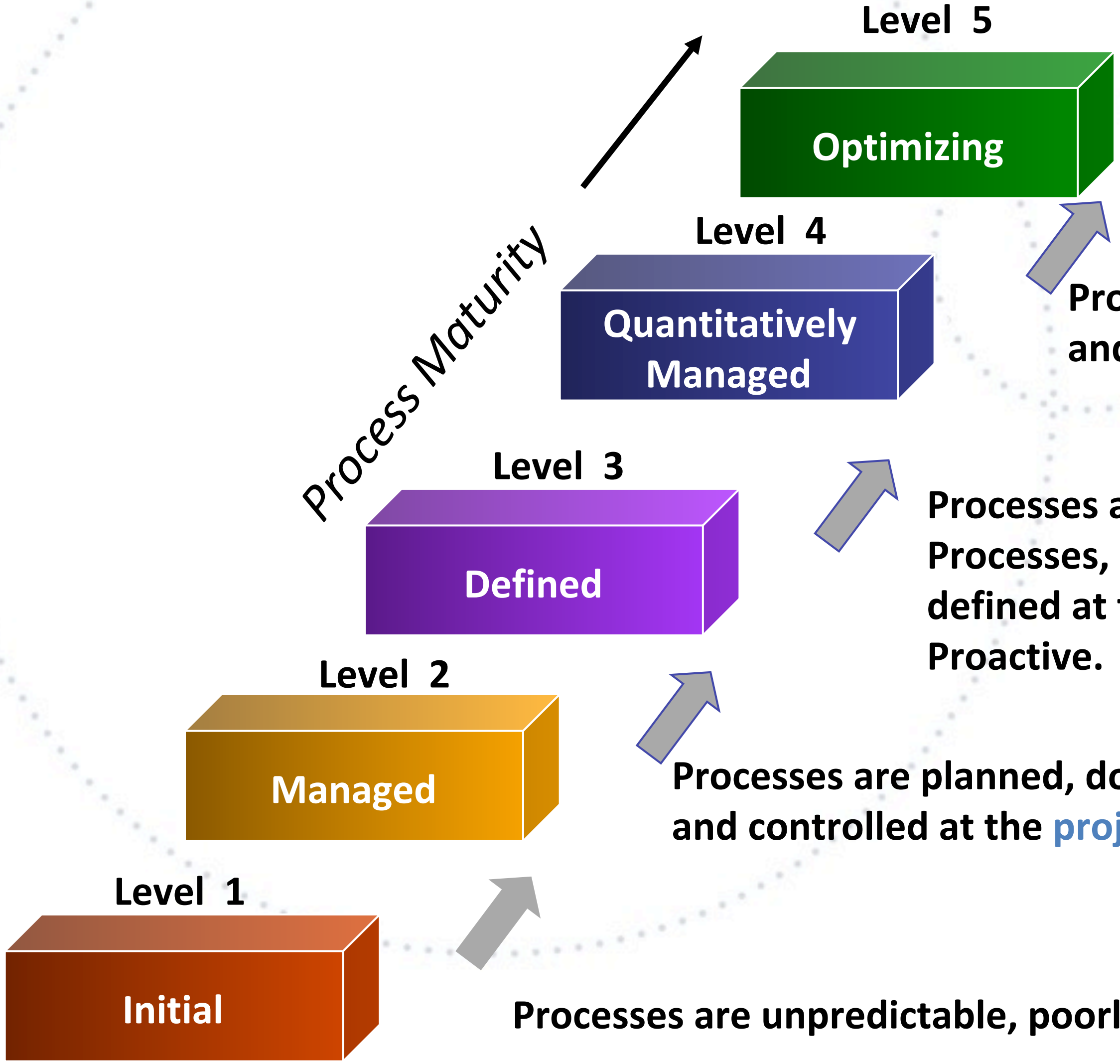
Security Assessment & Gap Analysis

- Capability Maturity Model (CMMI)
- Cybermaturity Platform

Capability Maturity Model Integration (CMMI)®

Cybermaturity Platform

CMMI – 5 Levels



Process Maturity

Level 5

Optimizing

Process performance continually improved through incremental and innovative technological improvements.

Level 4

Quantitatively Managed

Processes are controlled using statistical and other quantitative techniques.

Level 3

Defined

Processes are well characterized and understood. Processes, standards, procedures, tools, etc. are defined at the organizational (Organization X) level. Proactive.

Level 2

Managed

Processes are planned, documented, performed, monitored, and controlled at the project level. Often reactive.

Level 1

Initial

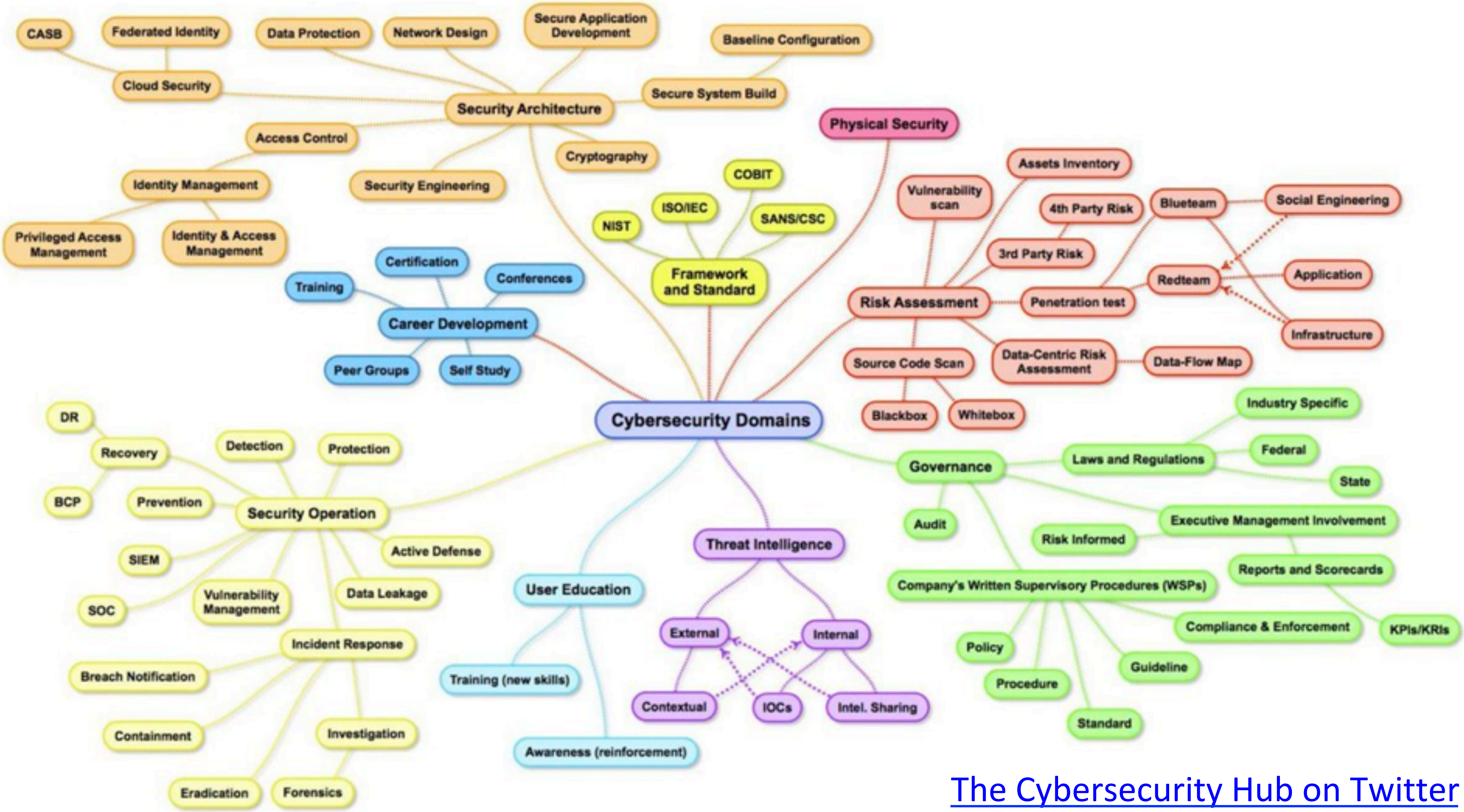
Processes are unpredictable, poorly controlled, reactive.

CMMI Institute

WTF-OMG Compliance

ISO
27001
AICPA Service Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports
GDPR
EU General Data Protection Regulation
COBIT® 5
AN ISACA® FRAMEWORK
NIST
PCI DSS COMPLIANT
HIPAA
CSA
cloud security alliance℠
PIPEDA
The Personal Information Protection and Electronic Documents Act

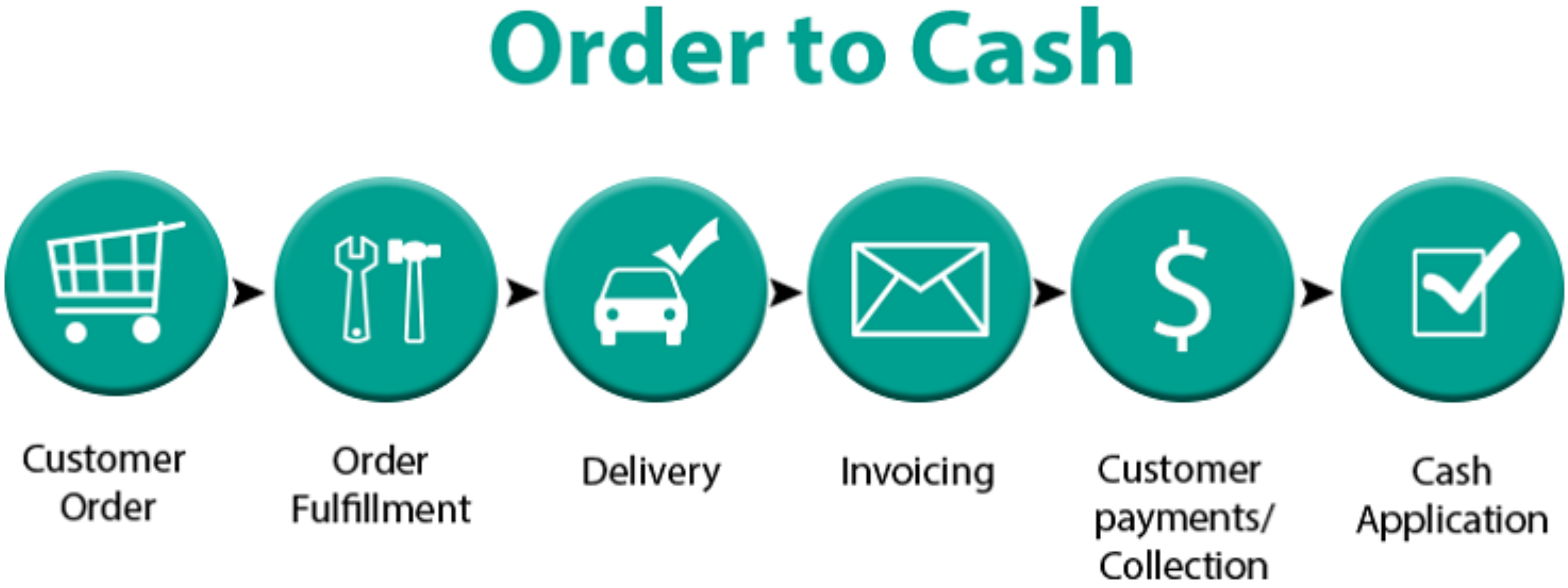
How and Where to Focus?



- Cybersecurity Domains
  - Security Architecture
    - Cloud Security
      - CASB
      - Federated Identity
    - Data Protection
    - Network Design
    - Secure Application Development
    - Secure System Build
      - Baseline Configuration
    - Access Control
      - Identity Management
        - Privileged Access Management
        - Identity & Access Management
    - Security Engineering
    - Cryptography
  - Physical Security
  - Framework and Standard
    - NIST
    - ISO/IEC
    - COBIT
    - SANS/CSC
  - Risk Assessment
    - Vulnerability scan
    - Assets Inventory
    - 4th Party Risk
    - 3rd Party Risk
    - Penetration test
      - Blueteam
      - Redteam
        - Social Engineering
        - Application
        - Infrastructure
    - Source Code Scan
      - Blackbox
      - Whitebox
    - Data-Centric Risk Assessment
      - Data-Flow Map
  - Career Development
    - Training
    - Certification
    - Conferences
    - Peer Groups
    - Self Study
  - Security Operation
    - Recovery
      - DR
      - BCP
    - Detection
    - Protection
    - Prevention
    - SIEM
    - SOC
    - Vulnerability Management
    - Active Defense
    - Data Leakage
    - Incident Response
      - Breach Notification
      - Containment
      - Eradication
      - Forensics
      - Investigation
  - User Education
    - Training (new skills)
    - Awareness (reinforcement)
  - Threat Intelligence
    - External
    - Internal
    - Contextual
    - IOCs
    - Intel. Sharing
  - Governance
    - Laws and Regulations
      - Industry Specific
      - Federal
      - State
    - Audit
    - Executive Management Involvement
    - Risk Informed
    - Reports and Scorecards
      - KPIs/KRIs
    - Company's Written Supervisory Procedures (WSPs)
      - Policy
      - Procedure
      - Standard
      - Guideline
    - Compliance & Enforcement

The Cybersecurity Hub on Twitter

Critical Business Processes



Apttus

Patch Management is Paramount!

National Library of Australia nla.pic-vn4728563-v

National Library of Austrailia

Data Inventory

- What, where, why, when & how
- Follow the data trail
- Backups
- End-user computers
- Storage media
- Archived applications
- What’s in the Cloud?

Data Classification

- Public, Internal, Confidential, Secret
- PII: Customer & Employee
- Defined Repositories
- Commensurate Security Levels
- Managed Data Life Cycle

Security Policy

- Compliance Driven
- Business Driven
- Ownership
- 3rd party
- Customer Input
- Training
- Controls Design & Mapping
  - Cloud Controls Matrix (CCM) - Cloud Security Alliance

Building Secure Foundations

61 - 90

Security vs Security Operations

DON'T MIND ME...
CISO
MD
SecOps

Wordpress

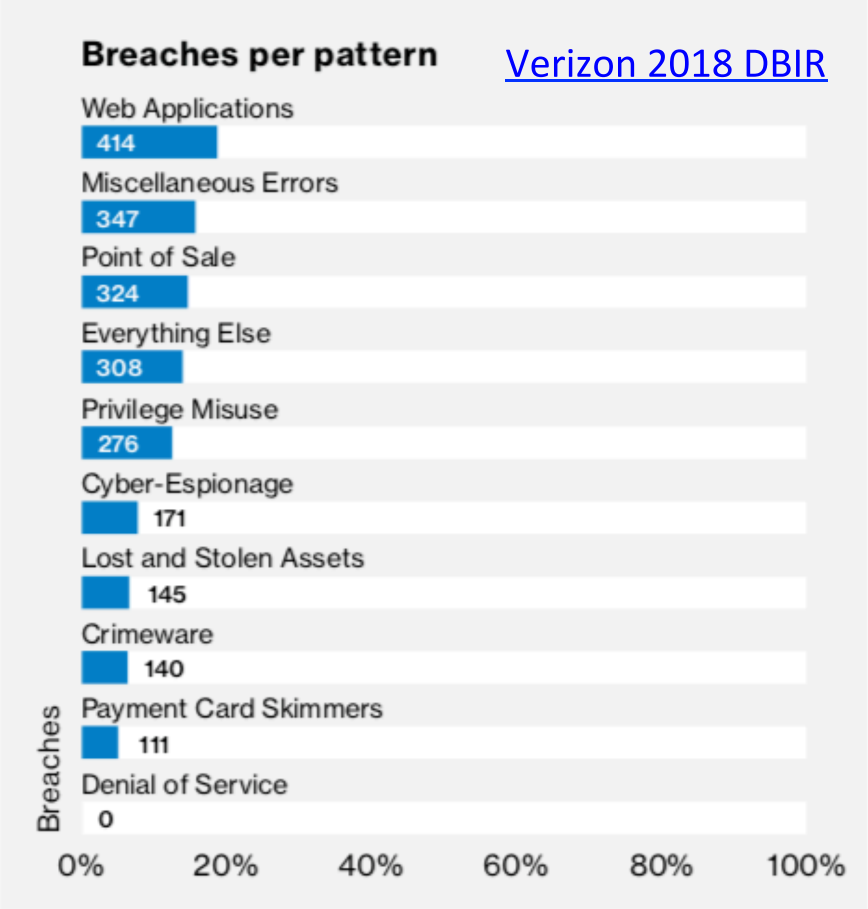
Security Awareness Training

- Business Unit Relevance
- Joint delivery with BU-ISO
- Compliance driven
- Sec-Dev-Ops Training
- Relevant 3rd Party training

Application Security

- Every company is a technology company
- In-house vs 3rd Party
- Secure SDLC
- Security Compass Training

OWASP Open Web Application Security Project your Webapp!



Verizon 2018 DBIR

Figure 27. Percentage and count of breaches per pattern (n=2,216)

Business Continuity

- Business Process Driven
- Disaster Recovery
  - – Defined RTOs & RPOs
- Backup Strategy
- Denial of Service
- Testing

Stepup IT

Prepare for the Worst

Data Breach Preparedness

- Breach Scenario Planning
- Table-top Exercises
- Decision Tree
- Detection & Logging
- Contact Lists
- Time-to-Notify
- Bitcoins?!

IN CASE OF EMERGENCY

BREAK GLASS

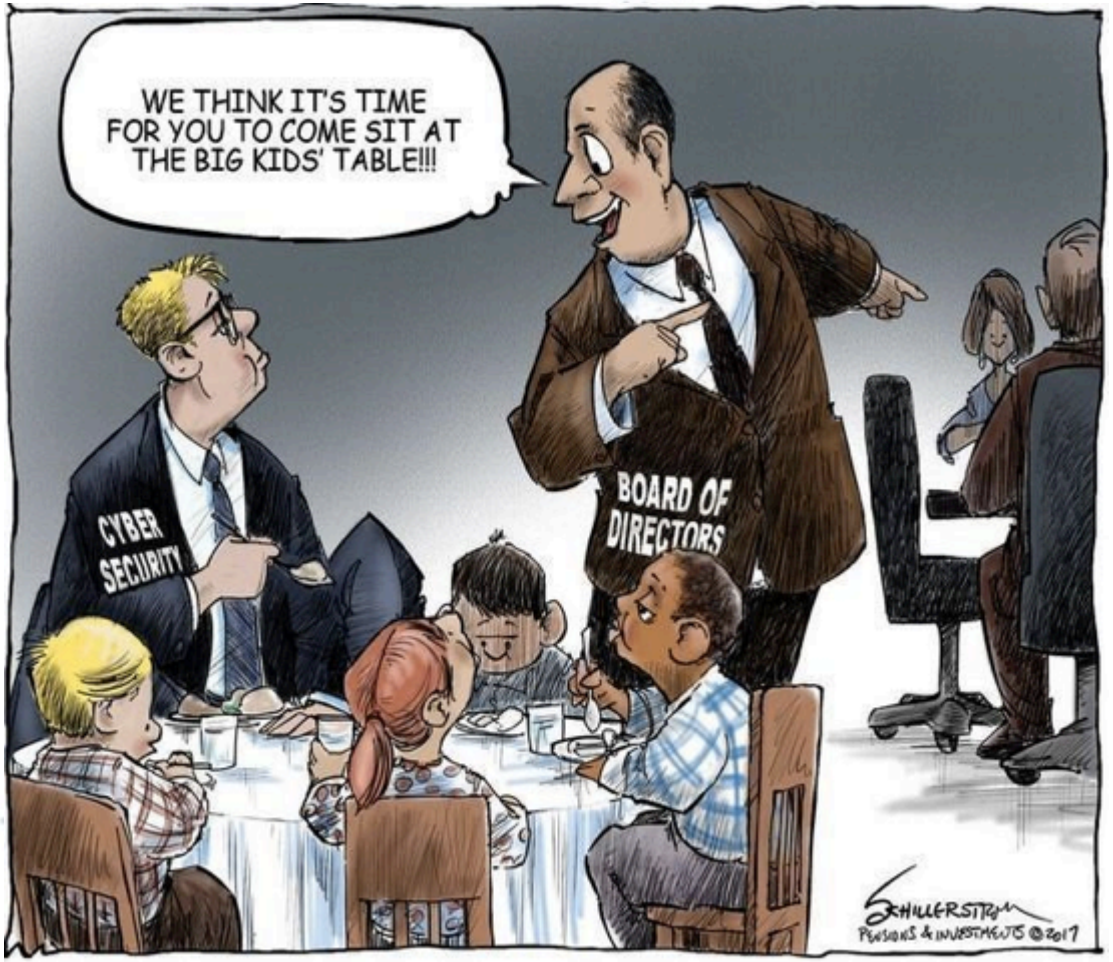
Data Breach Response Plan

Customer-Facing Security

- Securing Client Services
- Supporting Sales
- Customer Security Compliance
- Vendor Security Questionnaires
- Legal Agreements – Security Language

90+

Security is a Board-level Problem


WE THINK IT'S TIME FOR YOU TO COME SIT AT THE BIG KIDS' TABLE!!!
CYBER SECURITY
BOARD OF DIRECTORS
SCHILLERSTROM
PENSIONS & INVESTMENTS ©2017

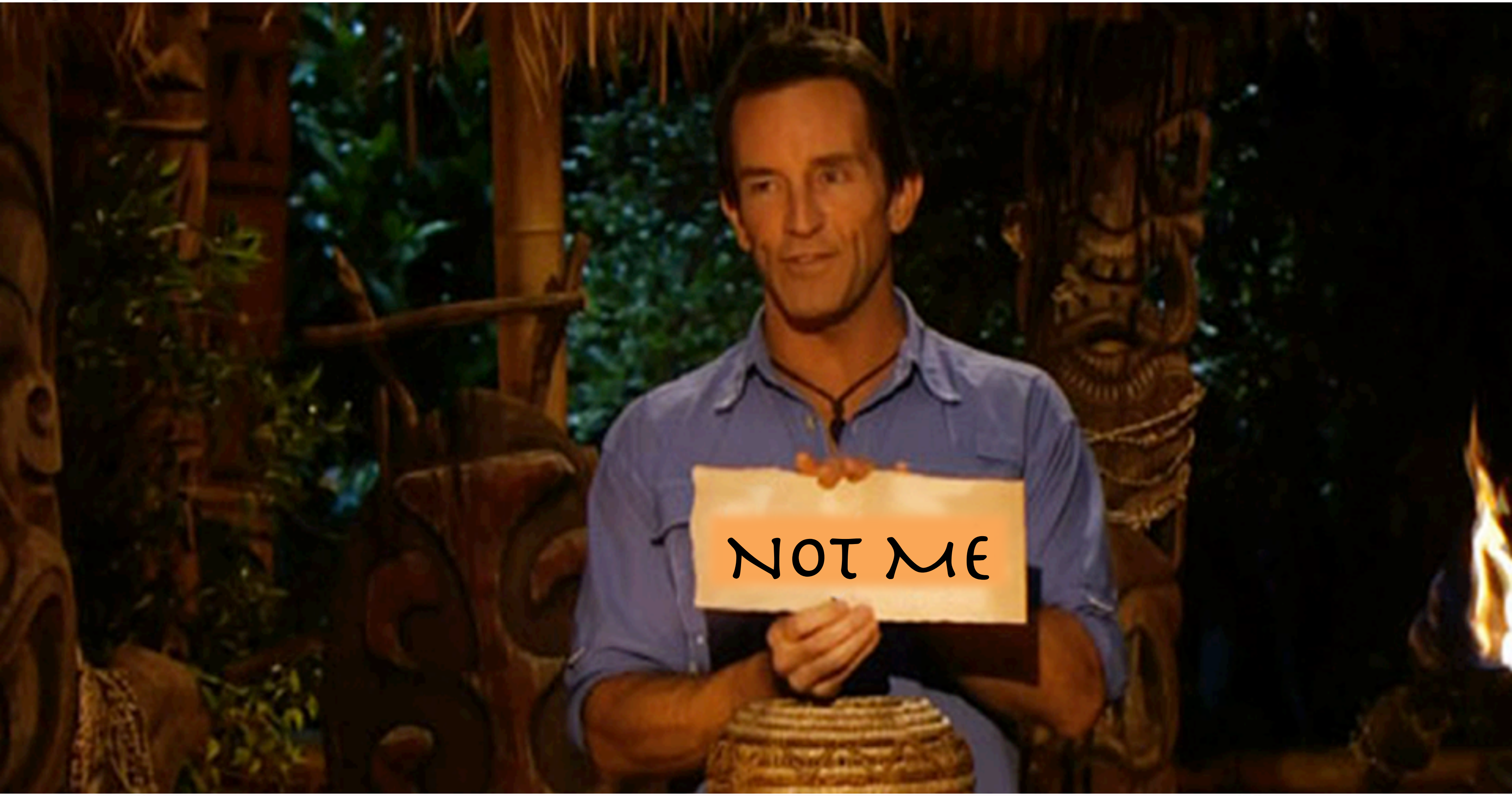
And a message from the

Office of the
Privacy Commissioner
of Canada

- On November 1, 2018, Data Breach Notification Laws will be enforced in Canada

KEEP CALM DO THE RIGHT THING AND CYA

The Tribe Has Spoken …



Chief I'm the Scapegoat Officer