New Age Enterprise Security Playbook: First 100 Days

Dominic Vogel
Chief Security Strategist, Cyber.SC

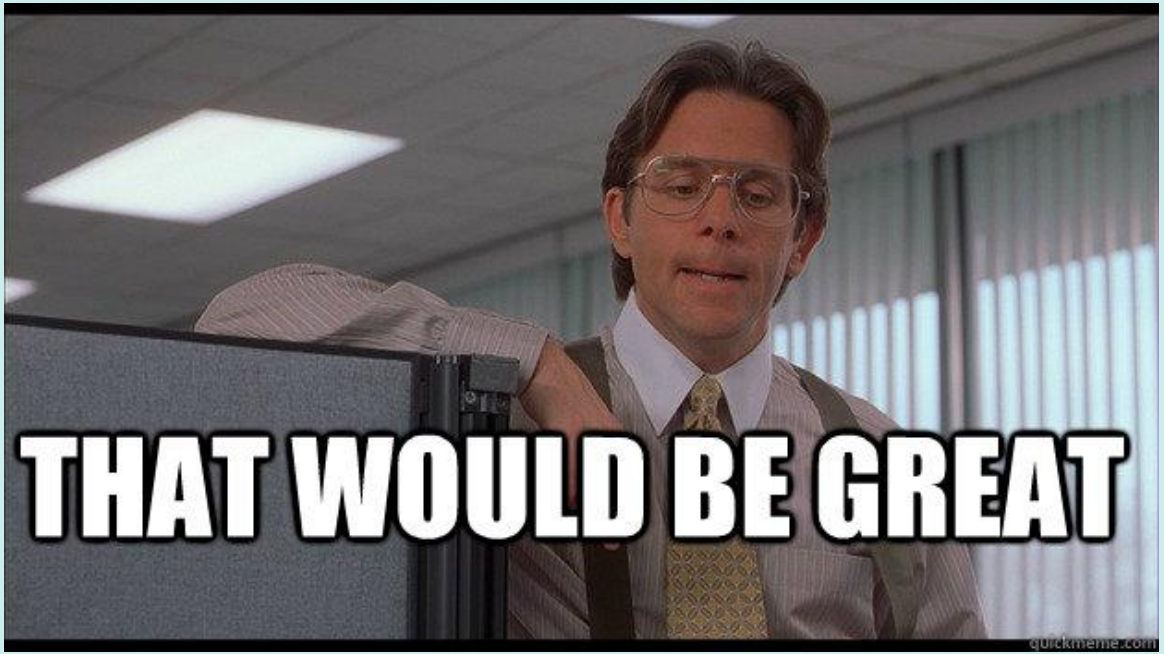
Who is this clown??

- Current:
  - Chief Security Strategist, Cyber.SC

- Previous:
  - Security Strategist (Contractor), Health Services Authority
  - Cyber Security Contractor, TELUS (BC Hydro)
  - Information Security Team Lead, First West Credit Union
  - Senior Security Consultant, Grant Thornton
  - Global Security Administrator, CHC Helicopter

- Frequent security commentator radio/TV/social media

Introducing: the Know-It All CIO



Effective Security: Five Pillars

- Create positive and effective security culture
- Make secure solution easier than non-secure business process
- Avoid knee-jerk reactions to security threats
- Develop risk-based security approach
- Foster enduring internal business relationships

Know-It All CIO – Security Culture

CIO: Everyone needs to complete the security awareness training except me because I am so damn brilliant

Me: I think we have different interpretations of the word “everyone”…and “brilliant”

Security Culture

- Create and foster organic culture
- Two pronged: top-down & bottom-up
- Positive attitudes
- Educate not shame
- Embrace humility

Discussion: Security Culture

Time to share!

- **Success (or horror!) stories**
- **Lessons learned**
- **Ingredients for success; pitfalls to avoid**
- **Questions & comments**

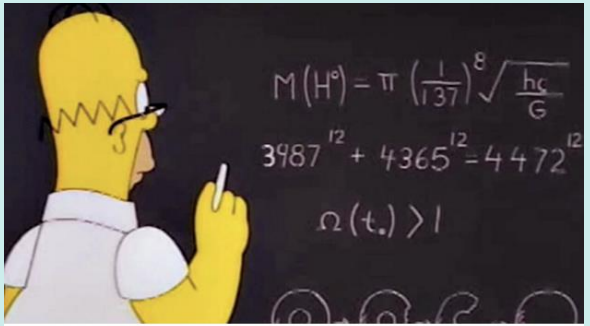
Know-It All CIO – Complexity

CIO: We need email encryption. Solution X does email encryption. Buy Solution X. Damn I’m handsome!

Me: (face buried in palms) I should go check my lottery tickets

Conquer Complexity

- Make secure solution easy
- Secure processes ignored otherwise
- Define business problem
- Gather business requirements
- Communicate with business leaders



Homer's insights into math and physics *Screenshot: Huffington Post/Fox*

Operations Complexity: Alert Overload

- Security is not “chasing alerts”
- Detection efficiency and accuracy
- Only 4% alerts typically investigated
- Focus on data value rather than volume
- Choose fewest number of key data sources

Discussion: Conquering Complexity

Time to share!

- **Success (or horror!) stories**
- **Lessons learned**
- **Ingredients for success; pitfalls to avoid**
- **Questions & comments**

Know-It All CIO – Knee Jerk Reactions

CIO: Block DropBox! Now we don't have to worry about data leaving to the cloud thingy….squirrel!

Me: Where is my bottle of aspirin?

Lowest Form of Life (other than Donald Trump)

If your security program is focused on reacting to news of the last data breach, you've all but ensured that you'll fall victim to the next data breach.

Cap the Knee-Jerk Reactions

- Focus building resilience (people, process, technology)
- Knee-jerk reactions more damaging
- Assess and solve problems holistically
- Stop focusing on the “threat du jour”
- Risk prioritization – important assets

Discussion: Knee-Jerk Reactions

Time to share!

- **Success (or horror!) stories**
- **Lessons learned**
- **Ingredients for success; pitfalls to avoid**
- **Questions & comments**

Know-It All CIO – Handling Risk is Easy!

CIO: I've told the board and the CEO that we have 100% security and that the risk of a data breach is zero. We are tighter than Fort Knox baby!

Me: You would have made an excellent grave-digger

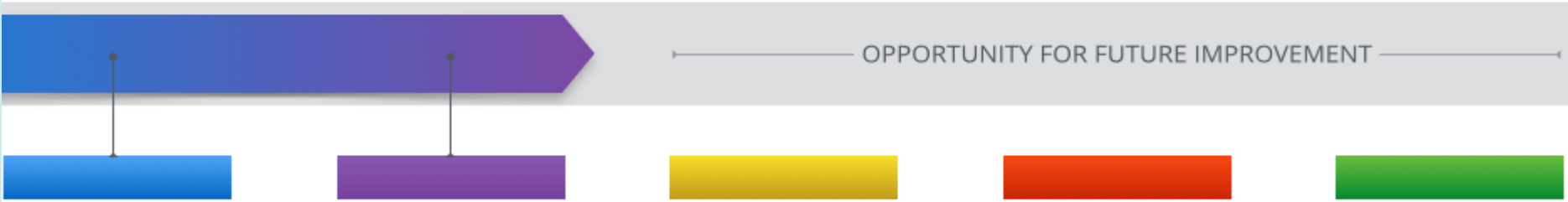
Risk-based Security – Governance Frameworks

- Frameworks provide the blueprint for building security
- Define & prioritize tasks
- Manage cyber risk intelligently
- Prevent a haphazard approach to information security
- Reduce potential gaps in security efforts

Risk-based Security – NIST CSF Framework

- High-level in scope; very concise
- Focuses on how to access and prioritize security functions
- Useful to achieve C-Suite buy-in
- Flexible in its implementation; combine with CIS Top 20
- Builds on (and does not replace) existing security standards

Risk-based Security – NIST CSF Framework



IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT

- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT

- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recover planning
- Improvements
- Communications

Risk-based Security

- Do not take the old school “theoretical” approach
- Focus on critical data assets (deliver high ROI)
- Achieving 100% risk free environment is impossible
- Standardize on value at risk model such as FAIR
- Executives provided with actionable data about cyber risks
- Outcome: increase in business and greater efficiency

Discussion: Risk-based Security

Time to share!

- **Success (or horror!) stories**
- **Lessons learned**
- **Ingredients for success; pitfalls to avoid**
- **Questions & comments**

Know-It All CIO – Relationships

CIO: Who gave you permission to speak to the VP of Operations? How dare you disobey the rigid hierarchy. I am the voice of security in this organization! You only speak when spoken to.

Me: Your fly is down…

Build Business Relationships

- Get out of your damn ivory tower (or boiler room)
- Drop “no” from your vocabulary
- Develop rapport as trusted business advisor
- Deliver effective and sustainable security

Discussion: Building Relationships

Time to share!

- **Success (or horror!) stories**
- **Lessons learned**
- **Ingredients for success; pitfalls to avoid**
- **Questions & comments**

Key Outcomes – Make Security Easy

- Overcome obstacle and break down silos
- Increase organizational resiliency
- Seamless collaboration
- Greater value for security dollars
- Increase in business and greater efficiency
- Cannot please everyone

Thank you! Any questions?

How to Contact Me…if you want…

- Email: dvogel@cyber.sc
- Twitter: @domvogel
- LinkedIn