Rule No. 1: Don’t Lie

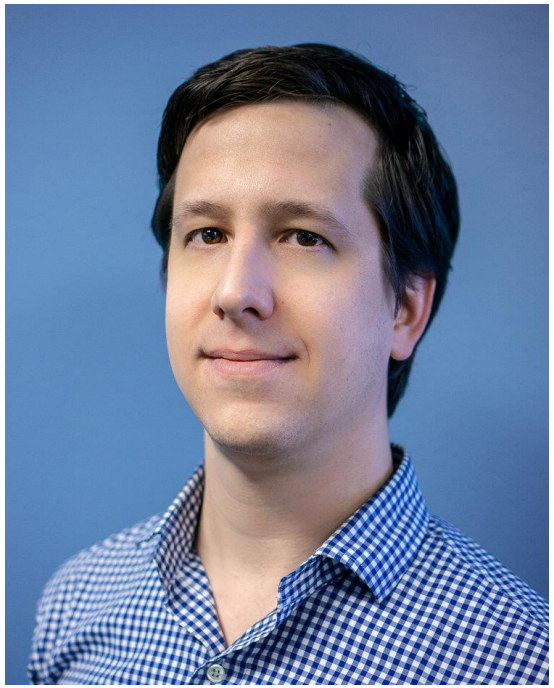
IT and Cybersecurity Compliance

Today's Agenda

- (Very) brief introduction
- Defining compliance
- A basic IT compliance framework
- Policy writing
  - Incident response
  - Remote working & Bring your own device (BYOD)

This is a highly interactive session, please ask questions as you think of them!

The slide where I talk about myself



Dustin Bolander

- Owned 2x IT/cybersecurity companies
- Cyberinsurance owner/consultant
- Technology background
  - Exchange & Active Directory
  - 10+ Microsoft engineering certifications

https://www.linkedin.com/in/dbolander/

Compliance in Legal

Client audits / requirements

Cyberinsurance

Bar opinions

Typical Client Audit

- Patching
- Security Officer
- InfoSec Policy
- Multifactor
- BYOD Policy
- Retention Policy
- Antivirus
- 24x7 SOC
- Network Use Policy
- Vendor Management
- Asset management
- Password policy
- Backup testing
- Encryption
- Incident Response
- Cyberinsurance
- Security Awareness
- Vulnerability Scans
- Software inventory
- EDR
- Logging & auditing

TOO MUCH!

Let’s simplify!

- Critical Security
  - Multifactor – everything external
  - Patching - <30 days for new critical issues
  - Security awareness training
  - Antivirus
    - Endpoint Detection & Response (EDR)
  - Secure remote access

- What about cyberinsurance requirements?

Let's simplify!

- Who, what, when, where, why
- Critical Policies
  - Security policy – what and why
  - **Incident Response (IR), Disaster Recovery (DR)**, Business Continuity

    …this can be one policy!
  - **Network use** – can include remote work, data handling, BYOD, social media
  - **Retention policy** (documents, matters, emails, etc.)

IT Policy Writing 101

- Incident Response
  - 1 page!
  - Who and when – assign roles, schedules (escalations, notifications, etc.)
  - After action…we'll do something (meeting)
- Disaster Recovery
  - What and how fast

IT Policy Writing 101

- Remote working / network use
  - What (devices allowed/BYOD, data handling) and when (communication and statuses)

- Retention policy
  - ~~Keep everything forever~~
  - Data = liability!
  - Different system = different retention