A Conversation with a CISO

What do you want?

Colleges and University Auditors of Virginia Conference 2024

OLD DOMINION UNIVERSITY

Conversation with a CISO

Hello, I'm a CISO, and this is what I wish you knew about cybersecurity:

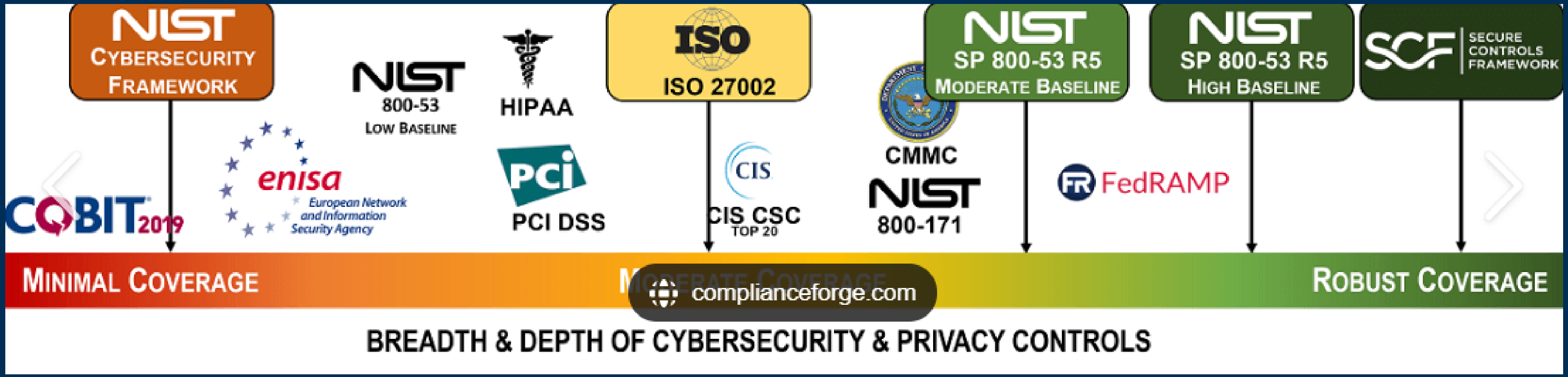
WHAT DO YOU WANT?

It’s Complicated: A wave of digital transformation

- Hundreds of internet accessible hosts
- Hundreds of applications and services
- Hybrid on-prem / cloud architecture
- Scores of 3rd party providers with sensitive information
- Thousands of desktops browsing the internet
- Remote privileged-access increasingly required
- Direct DB access, privileged accounts, distributed IT
- Constant social engineering attacks (& compromised credentials)
- Growing regulatory and compliance requirements
- 100s of network segmentation
- Enable research and business while supporting the mission of growing enrollment
- A committed adversary

It’s Scary:

“We’re not Fort Knox!”



NIST CYBERSECURITY FRAMEWORK

NIST 800-53 LOW BASELINE

HIPAA

ISO ISO 27002

NIST SP 800-53 R5 MODERATE BASELINE

NIST SP 800-53 R5 HIGH BASELINE

SCF SECURE CONTROLS FRAMEWORK

COBIT 2019

enisa European Network and Information Security Agency

PCI DSS

CIS CIS CSC TOP 20

CMMC

NIST 800-171

FedRAMP

MINIMAL COVERAGE

MODERATE COVERAGE

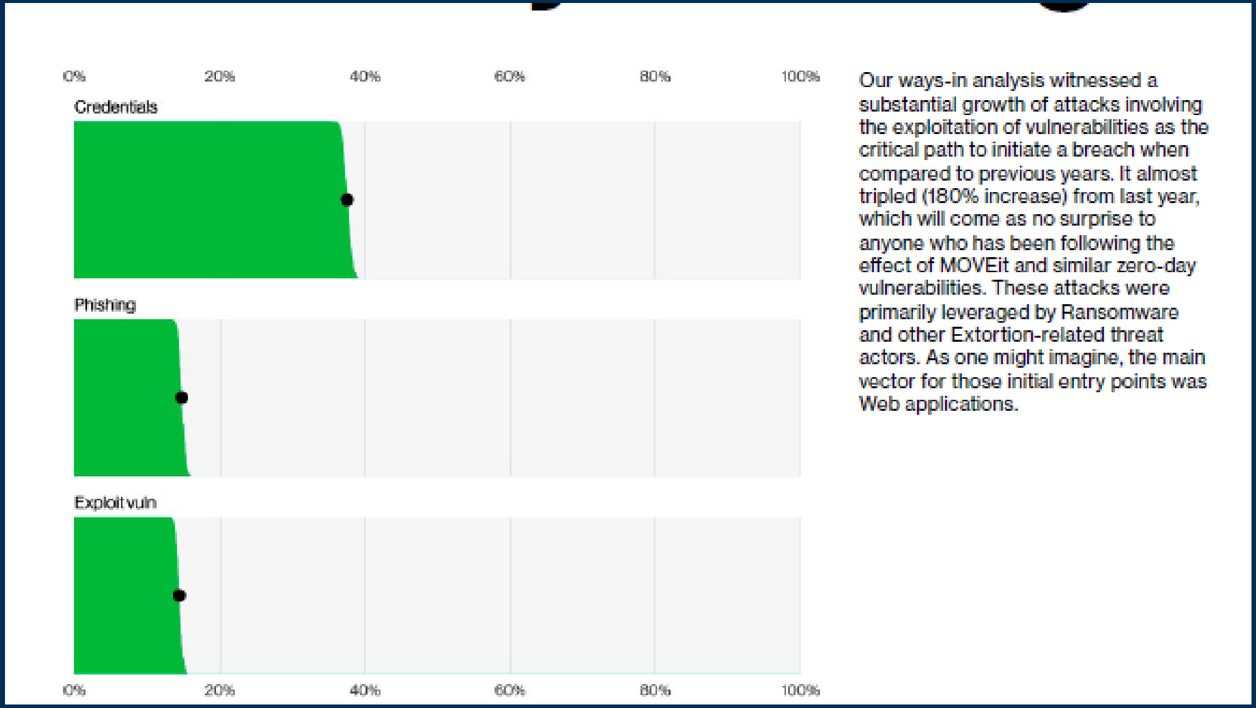
ROBUST COVERAGE

complianceforge.com

BREADTH & DEPTH OF CYBERSECURITY & PRIVACY CONTROLS

It’s Scary:

- “the worse ransomware year on record” after attacks spiked by 70%”
  - 105% increase in known ransomware attacks against k-12 and higher education.
  - [Cyberattacks on Higher Ed Rose Dramatically Last Year, Report Shows | EdTech Magazine]
- Employees, Students scammed out of $$ thousands
- Do you know anyone whose identity has been stolen?
- Researcher – years of work encrypted and stolen
- Hundreds of thousands student and parent/guardian PII with limited tools for archiving or minimizing, and growing



Our ways-in analysis witnessed a substantial growth of attacks involving the exploitation of vulnerabilities as the critical path to initiate a breach when compared to previous years. It almost tripled (180% increase) from last year, which will come as no surprise to anyone who has been following the effect of MOVEit and similar zero-day vulnerabilities. These attacks were primarily leveraged by Ransomware and other Extortion-related threat actors. As one might imagine, the main vector for those initial entry points was Web applications.

CISO perspective

It’s Scary:

- The top 5 impacts of cybersecurity breach
  - **Reputational harm**
    - Cybersecurity programs
    - Donor loss
    - Recruitment
  - **Theft** – identity, IP, Accounts ($15 per user, $3k for Domain Admin)
  - **Financial Loss** – Direct loss of funds, insurance premium increases, business down time, lost revenue, refunds, direct costs of response
  - **Fines** – GDPR, HIPAA, loss of Financial Aid distribution
    - Virginia is one of three states to institute comprehensive privacy legislation
  - **Hidden costs** – Productivity, lost man-hours, recovery, rearchitecting, added audit scrutiny, added assurance measures

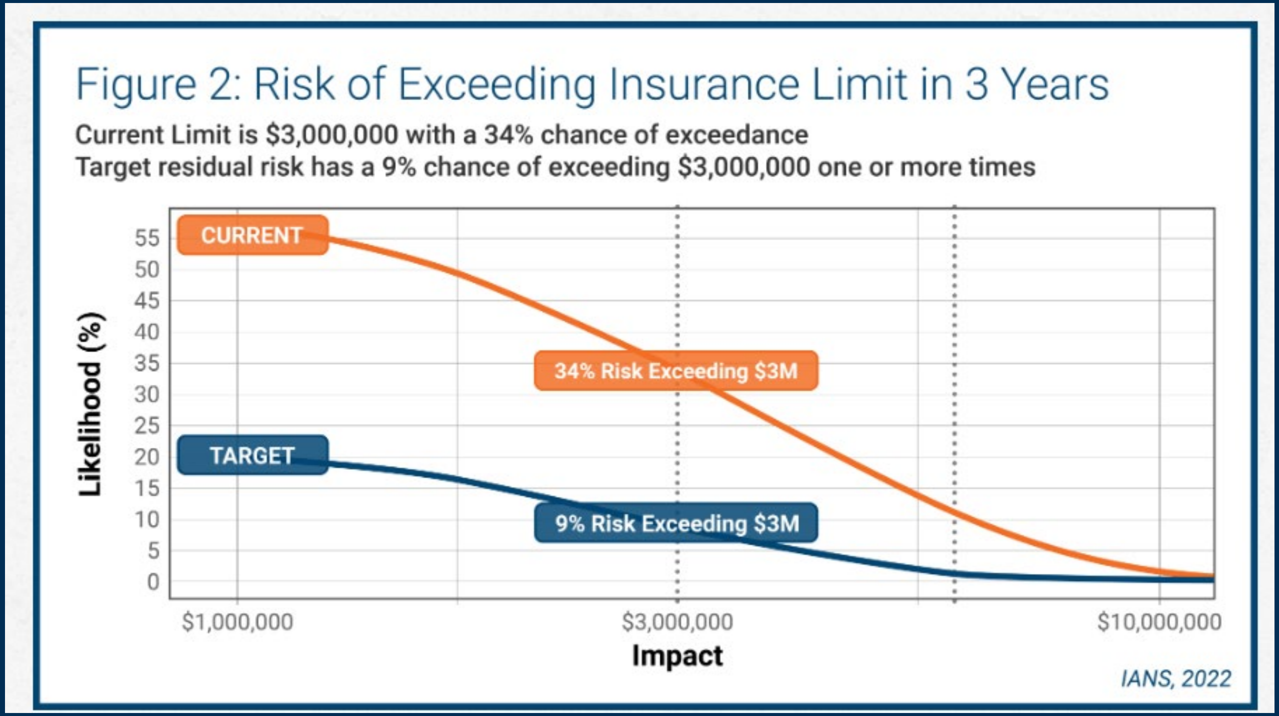


Figure 2: Risk of Exceeding Insurance Limit in 3 Years

Current Limit is $3,000,000 with a 34% chance of exceedance
Target residual risk has a 9% chance of exceeding $3,000,000 one or more times

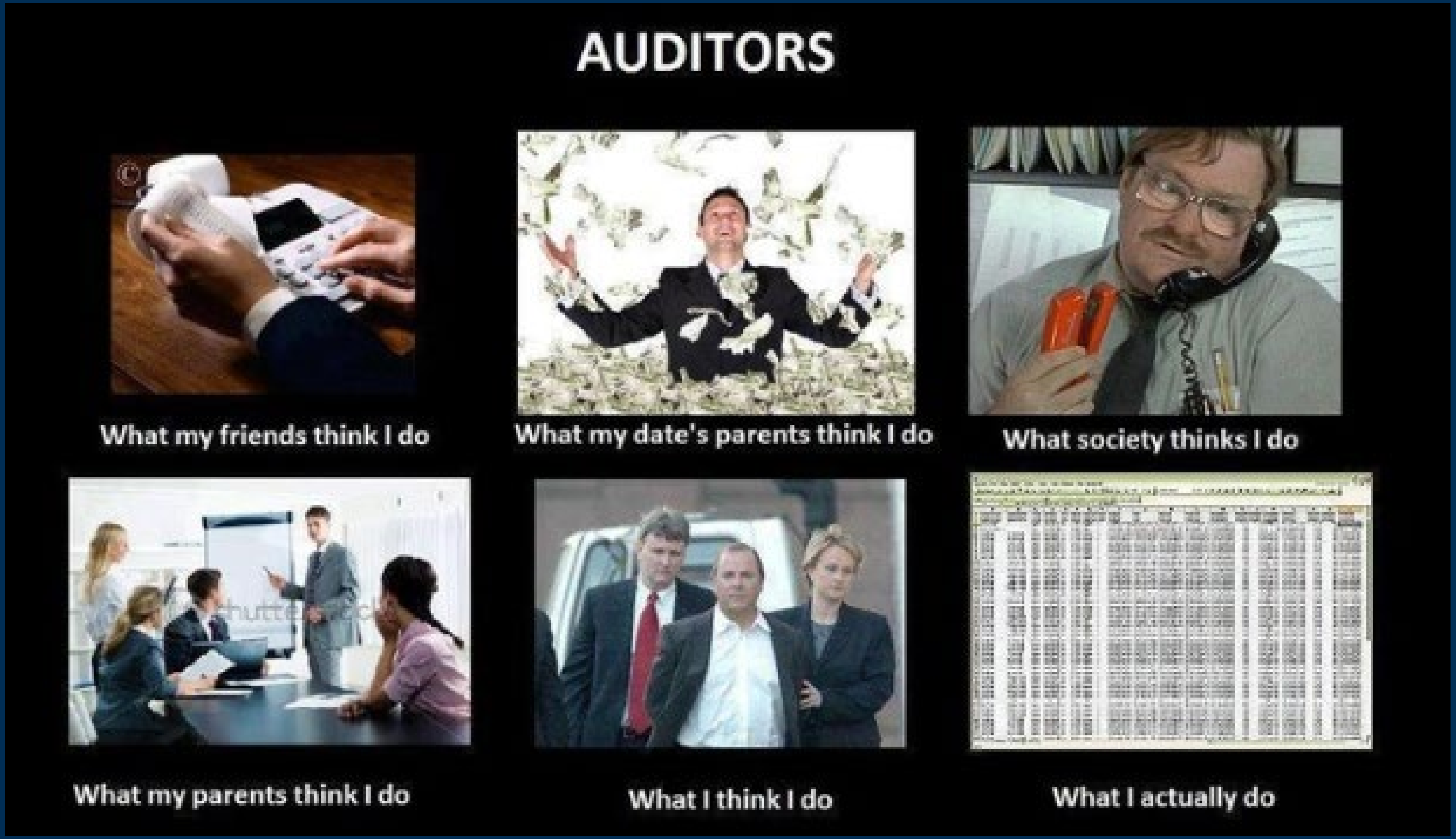
IANS, 2022

We cannot do it without you:

Maximize the benefits of a good Auditor relationship:

- Necessary to ensure our organization’s controls are in place and are functioning as expected.
- Simply doing your job
- Open Communication
- Accurate and honest
- Concise and specific

How do we work together?


AUDITORS
What my friends think I do
What my date's parents think I do
What society thinks I do
What my parents think I do
What I think I do
What I actually do

- Hunt for opportunities to partner with your Internal Auditors
  - Policy, standard, procedure improvements
  - Program, process improvements
  - Getting needed committees off the ground and seeking stakeholder buy in

WHAT DO WE WANT?

We want to talk:

- What do you need from an Information Security Program?
- Ensuring we understand the audit scope and objectives and ensure they align with the intended goals prior to fieldwork and control testing beginning
- Passing an audit doesn’t make you secure.
- Communication is key