aliv business

# CYBER SECURITY SUMMIT 2026

**CYBER RESILIENCE**
DEFENDING THE DIGITAL FRONTIER
EMPOWER, PROTECT, EVOLVE

## WHY ORGANIZATIONS WITH "GOOD COMPLIANCE" STILL GET BREACHED?

### Beyond the Checkbox

**Presenter Shervin Evans**
**Founder & CEO, 21st Century Cybersecurity**

# If We Passed the Audit, Why Were We Breached?

SOC 2 Compliant

ISO 27001 Certified

Clean Regulatory Report

No Major Audit Findings

...Yet Incident Response Triggered

**Compliance Gives Assurance. It Does Not Guarantee Resilience.**

# Compliance vs. Security (The Difference)

| Compliance | Security |
| --- | --- |
| Proves controls exist | Proves controls work |
| Periodic assessment | Continuous defense |
| Documentation heavy | Detection heavy |
| Minimum requirements | Adaptive posture |

**Compliance is a Snapshot. Security is a Movie.**

# Major Breaches in Compliant Firms

## Case Study: Target (2013)

PCI compliant at the time

Breach via third party HVAC vendor

40+ million card records exposed

## Lesson: Vendor Risk Maturity Gap

# Major Breaches in Compliant Firms

## Case Study: Equifax (2017)

Regulatory compliant environment

Unpatched Apache Struts vulnerability

147 million people affected

## Lesson: Patch Failure Despite Frameworks

Proof that certifications are not a guarantee of security, as seen in catastrophic failures at Equifax and Target.

# Seven Reasons Good Compliance Fails

1. Minimum baseline only
2. Controls documented not tested
3. Point in time audits
4. Perimeter overreliance
5. Weak detection
6. Human factor gaps
7. Third party blind spots

# The Audit Timing Gap

**Audits are:**

- Annual
- Scheduled
- Predictable

**Threat actors are:**

- Continuous
- Opportunistic
- Automated

Security must be continuous, not calendar-driven.

# The Minimum Baseline Problem

**Compliance asks:**
"Do you have a policy?"

**Security asks:**
"Does it work during a live attack?"

**Organizations often:**

- Write policies
- Perform annual reviews
- Train once per year

**Attackers Operate Daily.**

# The “Check the Box” Culture

**Common mindset:**

“We passed the audit.”

“We met regulatory requirements.”

“We are compliant.”

**Dangerous assumption:**

Compliant = Secure

**This is false.**

# Compliance Fatigue

**Security teams:**

- Spend months preparing audit evidence
- Produce documentation binders
- Respond to questionnaires

**But:**

- Little time for proactive defense
- Little time for adversary simulation
- Little time for resilience testing

# The Human Risk Factor

**Most breaches involve:**

Phishing

Credential theft

Social engineering

Business Email Compromise


Compliance Requires Awareness Training.
Security Requires Behavior Change.

# The Maturity Shift

**From:**

•Compliance-driven security

**To:**

•Risk-driven security

**To:**

•Threat-informed defense

**To:**

•Resilient enterprise architecture

# Key Takeaway for Leaders

Compliance protects reputation with regulators.

Security protects reputation with customers.

**You need both.**
**But you cannot confuse them.**

# Closing Statement

Organizations with “good compliance” still get breached because:

Compliance validates intention.

Security validates effectiveness.

Cybersecurity is not about passing audits.

**It is About Surviving Adversaries.**

**Shervin Evans,** Msc., C|CISO, CHFI, CEH, CTIA ECIH, CISE CBE, CIAM

***Founder & CEO, 21st Century Cybersecurity***

***https://21centurycs.io***

***sevans@21centurycs.io***

# Thank You!

The Eagle Eyes Of Cyber Threats