ComplyWise online

Rewards and Reality

The Unseen Cost of Cybersecurity Complacency in Accounting Firms

Presentation Overview

ComplyWise online

Agenda	Description
Time:	60 minutes
Agenda:	• Introduction (5 minutes) • The Great Cybersecurity Myth (5 minutes) • Inside the Criminal Mind: How Cyber Criminal Operate (10 minutes) • Why Ordinary People Become Cybercriminals (10 minutes) • The Real Risk for Accounting Firms (5 minutes) • From Reactive to Resilient (10 minutes) • Q & A (10 minutes)
Attendees:	• **ComplyWise online:** Luke Kiely (Found and Chief Information Security Officer)
Objectives:	• Expose the psychology and criminal tactics behind modern cyber threats by examining real-world cases and understanding how everyday individuals, including insiders, are drawn into digital crime. • Identify the cybersecurity blind spots within accounting and tax firms - from overreliance on compliance checklists to the underestimated risk of insider threats. Reframe security as a leadership and cultural requirement, not just a technical one. • Develop a proactive, behavior-driven security strategy that moves beyond compliance to resilience by implementing zero trust principles, cultivating a security-aware culture, and addressing both technical and human vulnerabilities.
Delivery:	Virtual

Summary

ComplyWise online

This presentation is not about firewalls or phishing emails. It's about the reality of cybercrime. I explain how it's committed, how it's enabled, and why the accounting profession is particularly vulnerable.

As a former law enforcement officer in Cyber Crime, I've sat across from people who stole significant sums of money without leaving the comfort of their own home or ever touching a weapon.

As a CISO, I now see how easily the same crimes can happen inside legitimate businesses enabled by ignorance, arrogance and a misguided belief that compliance is enough.

This session aims to challenge what the audience think they know about cybersecurity. And it may just change how they lead their firm.

The Great Cybersecurity Myth

ComplyWise online

Firms don’t get breached because hackers are brilliant. They get breached because people assume someone else is responsible.

I tear down the illusion that:

- Cyber insurance is a safety net
- Compliance equals safety
- The assumption your IT vendors are handling “all things security”

Highlight:

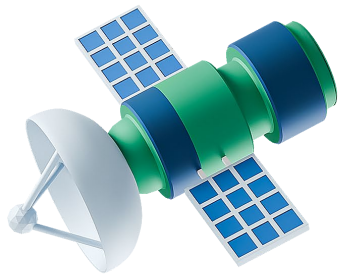
- The false sense of security driven by marketing and regulatory minimums.
- How firms outsource accountability, not just technology.

Inside the Criminal Mind

How Cyber Criminals Operate

From my law enforcement experience:

- Describe real cyber crime operations including how they're organized and what they look for.
- Debunk the idea of "genius hackers." Instead, it's low-tech, high-psychology.



Break down:

- **Social engineering**: How criminals groom and manipulate staff.
- **Reconnaissance**: How they study firm websites, staff LinkedIns, vendor portals.

Key Point:

Cybercriminals don't hack your systems - they hack your people.

Why Ordinary People Become Cyber Criminals

ComplyWise online

I've arrested people who said, "I just needed to pay my bills". They weren't villains. They were an everyday person who took a chance.

I deliver an input on insider threats and digital temptation based my experience in criminal investigations and security policy perspectives.

- Explain the Fraud Triangle: how ordinary employees commit digital crimes.
- Share stories: a call centre staff who stole credit card numbers. A contractor who leaked credentials. An admin who installed keyloggers "just to see."

Introduce the modern cybercrime economy:

- Online groups buying/selling login data.
- Deepfake voice impersonation
- "I didn't think anyone would notice" as the most common last words.

Insight:

The next breach mostly likely won't come through your firewall. It will come through a compromised login or an employee with a grudge.

The Real Risk for Accounting Firms

ComplyWise online

Criminals exploit the cracks between your people and departments, not just your endpoints.

I explain

- Why accounting firms are a top-tier target (PII, financials, tax data, access to client systems).
- The hidden vulnerabilities: Shared drives, outdated access control, cloud tools with default settings, the assumption your managed service provider is doing all your security.
- **Human layer** (email behavior, admin access)
- **Technology layer** (shadow IT, SaaS risk)
- **Process layer** (what happens after an incident)

Where Compliance Leaves You Exposed

Here, I draw the line between:

- Regulatory minimums (e.g., FTC Safeguards Rule)
- And security reality

And explain:

- How firms pass audits but still fail in real-world attacks.
- Why cyber insurance claims are being denied due to “gross negligence” or poor controls.
- How vague language in frameworks leads to false assumptions.

Insight:

Compliance is the floor. Criminals operate at the ceiling.

From Reactive to Resilient

I shift to empowering the audience:

Point 1: Risk Reframing

- Stop asking “Are we compliant?”
- Start asking: “What happens if we lose access to our systems for 5 days?”

Point 2: Culture vs Controls

- Make cybersecurity a performance metric, not just a training module.
- Foster a “see something, say something” culture.

Point 3: Zero Trust, Zero Excuses

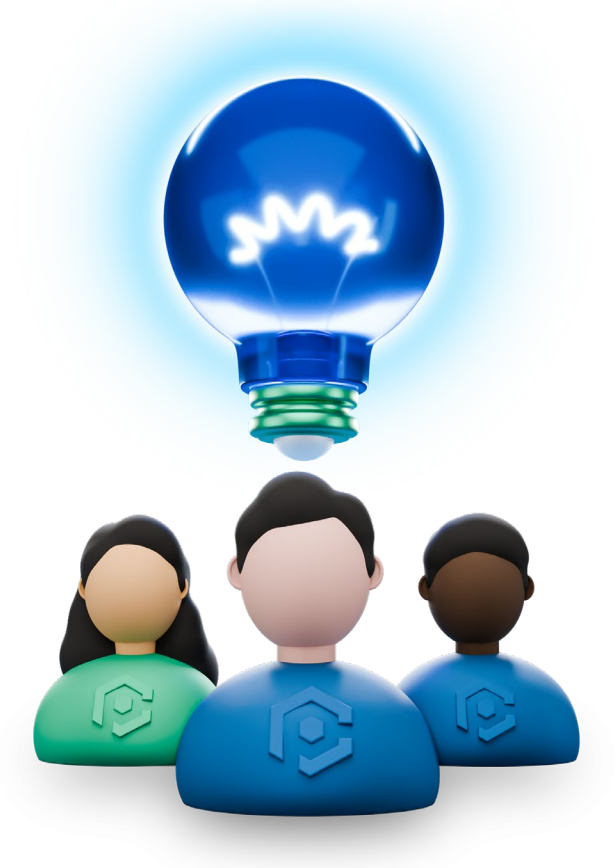
- Implement behavioral access controls, not just password policies.
- Review vendor access, API permissions, and system logs quarterly.

Don’t chase perfection. Chase visibility.

What’s the Real Reward

Leave the audience with:

- A challenge: What would your staff do in a crisis — and how do you know?
- A truth: The cost of getting it wrong is no longer just financial. It’s existential.
- And an opportunity: You don’t have to become a CISO — but you do have to start thinking like one.



Questions and Answers

ComplyWise online

An opportunity to discuss any aspect of this presentation or questions from the audience.