

# Digital Battleground for the Modern Firm

Luke Kiely

Chief Information Security Officer &  
Former Cyber Crime Officer

ComplyWise online™2025



# Presentation Overview

Agenda	Description
Time:	60 minutes
Agenda:	<ul style="list-style-type: none"><li>• Introduction (5 minutes)</li><li>• A Story You Can Relate To (5 minutes)</li><li>• Cybersecurity Compliance For Accounting Firms (5 minutes)</li><li>• Why Businesses Fail To Act (5 minutes)</li><li>• Modern Warfare Isn't Just Physical – It's Digital The Real Risk for Accounting Firms (5 minutes)</li><li>• What Is a Hacker? (5 mins)</li><li>• Phishing, Malware, Ransomware (10 minutes)</li><li>• Should You Pay a Ransom? (5 minutes)</li><li>• What Is a Cybersecurity Plan (10 mins)</li><li>• Q &amp; A (5 minutes)</li></ul>
Attendees:	<ul style="list-style-type: none"><li>• <b>ComplyWise online:</b> Luke Kiely (Found and Chief Information Security Officer)</li></ul>
Delivery:	Virtual

# Who I am & Why This Matters

- CISO advising accounting and financial firms
- Former cyber crime officer — I've hunted and criminally investigated the hackers who target you
- I help firms stay off the front page for the wrong reasons
- I'm here because accountants are under siege — and the enemy is digital, relentless and already inside.



# A Story You Can Relate To

“Jimmy” ran a mid-size CPA firm with over 500 clients. One spoofed email, one missed flag, and \$60,000 vanished in minutes.

- What happened?
- Why it keeps happening?

This wasn't bad luck. It was a failure in culture, process and accountability.

- ❌ Bad luck didn't steal \$60K.
- ❌ Bad strategy did.



# Cybersecurity Compliance For Accounting Firms

## FTC Safeguards Rule

Requires accounting firms handling consumer financial data to develop, implement, and maintain a **Written Information Security Program (WISP)**

## Data Privacy Regulations

Firms must comply with **federal and state privacy laws**, including the GLBA, the Right to Financial Privacy Act, and state-specific legislation like the **California Consumer Privacy Act (CCPA)** — especially when handling sensitive client data.

## Incident Response & Notification

Firms may be subject to **regulatory notification requirements**, including **prompt breach reporting** to affected parties and authorities.




# Why Business Fail To Act

- **Complexity:** “We don’t know where to start”
- **Cost:** “We’ll invest if something happens”
- **Complacency:** “We’re too small to be targeted”
- **Awareness:** “We didn’t know what we didn’t know”



# Modern Warfare Isn't Just Physical – It's Digital

- **2010 – Stuxnet:** A nation-state cyber operation crippled Iran's nuclear program by sabotaging centrifuges, all without firing a single missile.
- **2022 – Ukraine:** Cyberattacks took down government and financial systems just hours before military invasion — softening targets and spreading confusion.
- **2023 – Israel/Gaza Conflict:** Widespread DDoS attacks hit media, energy, and logistics sectors in an attempt to disrupt public communications and infrastructure.
- **2024 – Global Espionage:** Chinese APT groups breached telecom and law firms across the U.S. and Australia, extracting sensitive economic and defense data.

 You're not a bystander. You're a target, deliberately or collaterally.



# What is a Hacker?

**Forget the hoodie. Forget the basement.**

A hacker is any individual or group exploiting systems for personal, political, or financial gain. That includes:

- **Criminal syndicates** running ransomware-as-a-service
- **Insiders** leaking or stealing data
- **Nation-state actors** targeting industries to disrupt economies
- **Script kiddies** using prebuilt tools they barely understand

Hackers shouldn't be defined by appearance — they should be defined by **intent, capability, and opportunity**



# Phishing

The number #1 method of compromise globally

- It's emotional engineering: stress, urgency, fear, reward
- Tax season is open season for phishing
- Not just emails: SMS, websites, QR codes, and instant messaging



# Malware

- Malware = malicious software
- Delivery via phishing, drive-by downloads, infected attachments
- It adapts like a virus — polymorphic, stealthy, targeted
- Used for spying, stealing, destroying



# Ransomware = Data Hostage Crisis

- Delivered via phishing, malicious links, or exploit kits
- Encrypts files, locking you out of your own data
- Demands ransom, often in cryptocurrency, to unlock data
- Evolves constantly — stealthy, automated, and tailored to your environment
- Used to cripple operations, extort money, and damage trust

💡 It's not just malware — it's a business model.



# Should You Pay a Ransom?

**Short answer:** No

**Real-world answer:** It depends

Paying a ransom is discouraged, and may even be illegal, but the decision is rarely simple.

What to consider:

- Can you afford the operational downtime
- Do you have the right backups?
- Are you committing a criminal offence?
- Will your insurer cover the payment or recovery?



# What is a Cybersecurity Plan?

It's more than a checklist. It's a strategy for:

- Identifying your assets
- Understanding your risks
- Applying the right technology, processes, and training
- Preparing for the worst so you can recover your best



# Questions and Answers

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

