Keeping Pace With Cyber Risk

Your Clients' Trust, Your Firm's Future.

Christian Toon, Legal Sector Cyber Security Advisor 25th November 2024

CYBER | TECHNOLOGY | ARTIFICIAL INTELLIGENCE

Alvearium Associates

Briefing **OPERATIONS LEADERS**



The Perfect Storm

The sensitive nature of client data we hold The high-value financial transactions we process The potential for accessing confidential information

Cyber requirements from clients Partner expectations to protect profit SRA, The Law Society, The Bar – as well as NCSC and ICO

Alvearium Associates





Threat Landscape

Financial threats: The primary threat comes from cybercriminals seeking financial gain through theft of client funds or sensitive information.

Ransomware attacks: Increasingly sophisticated and automated ransomware attacks target vulnerabilities in law firms' systems.

Phishing and social engineering: Criminals use tactics like email phishing, voice phishing (vishing), and deepfake technology to impersonate clients, key roles, or witnesses.

Data breaches: Law firms are at risk of both external attacks and internal errors leading to unauthorized access to sensitive client information.

Alvearium Associates





Threat Landscape

Supply chain vulnerabilities: Cybercriminals may target law firms through less secure third-party vendors or cloud services.

Insider threats: Disgruntled employees or those with malicious intent pose a risk to data security.

State-sponsored attacks: Some law firms have been targeted by foreign governments seeking to disrupt economic activities or gather intelligence.

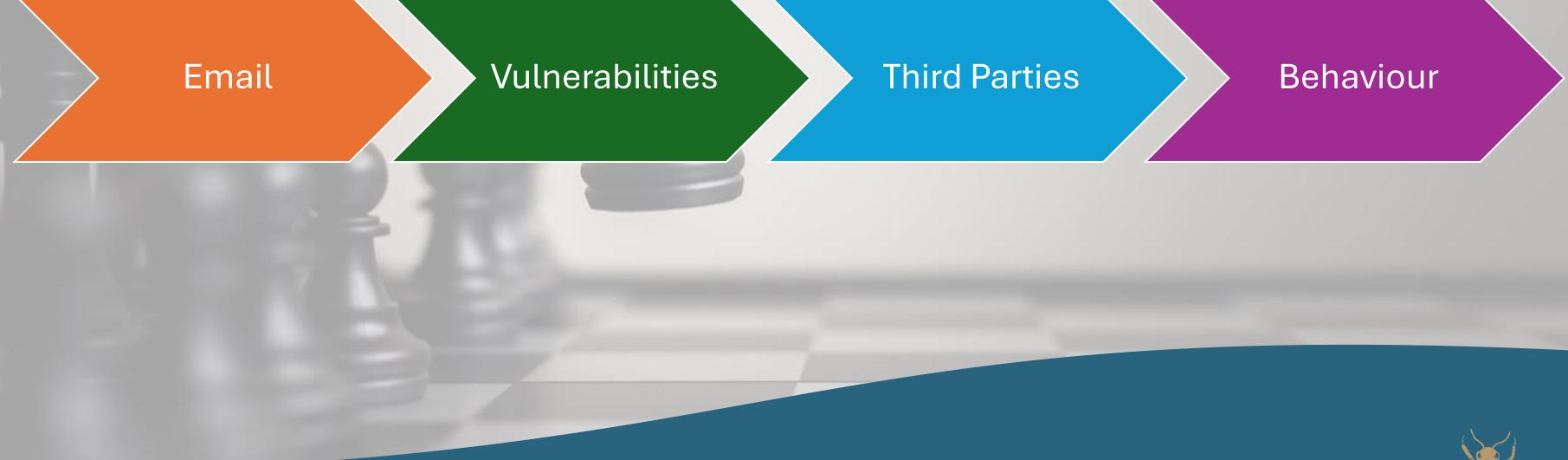
Al-powered attacks: Cybercriminals are increasingly using artificial intelligence to enhance their attack capabilities.

Alvearium Associates





Attack Vectors



Alvearium Associates





Protection Strategies

Appropriate Technical and Organisational Measures (ATOMs):

- Technical Controls
- Administrative Controls
- Operational Controls
- Detective Controls
- Third Party Controls





Incident Response

1.Immediate Actions 1.Isolate affected systems 2.Notify key stakeholders **3.Engage incident response team** 4.Contact cyber insurance provider 2. Critical Decisions

CYBER | TECHNOLOGY | ARTIFICIAL INTELLIGENCE

Alvearium Associates

1.Client notification requirements 2.Law enforcement engagement **3. Public relations strategy 4. Business continuity activation**





Recommendations

- Compliance is only good when your only threat is the Auditor.
- Threat based control response.
- Standards win you business, good security culture can help keep it.
- IR Plan, IR Plan, IR Plan
- Good Partners

Alvearium Asso



Questions



Alvearium Associates







