Integrity360

your security in mind

Q&A follow-up

Organised cybercrime: Inside modern threat adversaries

May 21st, 2026

1. Question: **Since QR-code phishing often shifts the attack to mobile devices outside traditional endpoint visibility, what defensive gaps should organizations be most concerned about?**

   Answer: From an organised cybercrime perspective, QR phishing creates several defensive gaps. Many organisations still have limited monitoring and detection capabilities on mobile devices compared to traditional endpoints, and QR based attacks can bypass email security controls because the malicious link is embedded in an image. Another concern is the blending of personal and corporate device usage. Employees may scan malicious QR codes on personal phones but still enter corporate credentials or approve MFA requests linked to business systems. Organised cybercrime groups are increasingly using QR phishing or other out of band phishing techniques because it scales well within social engineering campaigns and redirects victims to convincing mobile focused phishing infrastructure. The biggest risks for organisations are reduced visibility, weaker mobile security controls, credential theft, MFA abuse, and attacks occurring outside traditional monitoring environments.

2. Question: **Would making it illegal for companies to pay ransoms, reduce the revenue of criminals and reduce this crime?**

Answer: Making ransom payments illegal could reduce the profitability of ransomware, but it is unlikely to stop the problem entirely. Ransomware is fundamentally a business model, and organised cybercrime groups are highly adaptable. If payments become harder, many groups may shift toward other forms of monetisation such as data theft, fraud, extortion, or selling stolen access. This also poses practical and ethical challenges, especially for organisations facing severe operational disruption, or where the impact of not paying may have knock on effects to 3rd parties, such as medical records being leaked. Another concern is that payment bans could discourage transparent incident reporting, reducing valuable intelligence sharing with law enforcement and industry partners, thereby creating underground payment processes. Ultimately, this would reduce ransomware requires a broader strategy involving stronger preventative controls, resilience, coordinated law enforcement action, cryptocurrency tracing, and better intelligence sharing.

3. Question: **What are the major gaps identified when onboarding the customer or what challenges been observed while getting the customer onboarding?**

Answer: Most customer onboarding processes are now conducted remotely or through digital platforms, creating increased opportunities for impersonation, social engineering, and interception. As a result, organisations are required to perform onboarding activities across inherently untrusted communication channels. Strengthening onboarding security controls often introduces additional friction into the customer experience, requiring organisations to carefully balance security, usability, and operational efficiency. Establishing and continuously validating customer identity, not only during onboarding but throughout the entire customer interaction lifecycle, remains a longstanding and complex challenge for organisations. Increasingly, the most effective approach is likely to involve a layered or mixed authentication model that combines multiple verification mechanisms and contextual risk signals. The more seamlessly organisations can integrate multiple authentication and verification channels into the customer journey, without negatively impacting the user experience, the greater their likelihood of successfully addressing this challenge.