We Need to Talk About Organized Cyber Crime. It's Hurting You.

In recent years, we've seen a startling development in the e-crime ecosystem. It's not what you might expect. Cyber criminals are starting to buy Rolex Submariner watches and iconic Lamborghinis with personalized plates. They're spending on luxury brands and living lavish lifestyles.

But that's just the beginning. The reason for the lifestyle transformation? Cyber criminals are bringing in more bountiful cash hauls than ever before—via organized cyber crime.

Key facts: What is organized cyber crime?

- Organized cyber criminals maintain hierarchical business structures that resemble those of regular startups or Fortune 500 companies.
- Some organized cyber criminals operate international cyber crime syndicates, with partners and employees scattered throughout nations around the world.
- Organized groups of cyber criminals exploit new software vulnerabilities or technologies at lightning speed.
- In contrast with lone-wolf cyber criminals, organized cyber hackers have gained reputations as easy-to-pay and as entities with surprisingly good "customer service".
- Some are sophisticated enough to maintain their own research and development teams, project managers, specialists, money launderers and sales people.

Key issues: Organized cyber crime

- Are these organized cyber criminal syndicates becoming 'too-big-to-fail?'
- Leadership is usually well-established, and groups attempt to insulate those in leadership roles from detection, sanctions and prosecution.
- While cyber criminal motives range, some organized cyber criminal entities can be seen as terrorist organizations.

Cost of organized cyber crime

In terms of specific numbers, online fraud perpetrated by Central European crime networks leads to the defrauding of US citizens and entities at a rate of roughly $1 billion per year.[1]

Globally, networks of cyber crime syndicates cause an estimated $445-600 billion in harm per year.[2]

1 Transnational Organized Cyber Crime: A Growing Threat to National and International Security, The White House, President Barak Obama
2 Organized Cybercrime—Not Your Average Mafia, Science Daily, January 16, 2020

Examples of organized cyber criminal exploits

1. In 2021, the REvil ransomware crime group pulled off an unprecedented supply chain attack that ultimately affected more than a thousand organizations. Businesses affected included railways, pharmacy chains, and hundreds of grocery store franchises.

2. Across several years, the MageCart hacking group managed to disrupt Ticketmaster's UK operations, at least one airline, an electronics retailer, Shopper Approved, Topps sports collectable website, the Atlanta Hawks fan merchandise online store, hundreds of college campus bookstores, and NutriBullet, among other businesses.[3]

3. In 2018, a group of organized cyber criminals, known as the Cobalt Group, went on a hacking spree that targeted financial organizations. The group is believed to have struck banks in more than 40 countries, potentially acquiring as much as €10 in profits. After all was said and done, the group caused **over a billion** in damages.[4]

How to prevent attacks

In many ways, preventing organized cyber crime is similar to preventing old-school organized crime.

- **Educate your employees around key issues.** Make information easily comprehensible. Avoid technical jargon. Ensure that messages are tied into employees' day-to-day activities and that their own stake in security outcomes remains readily apparent. Consider a diversified communications strategy that includes workshops, Q&A sessions, video programming and emails, making cyber security an ongoing conversation.

- **Enhance your intelligence and information sharing.** As the internet continues to grow and evolve, reactive strategies for contending with cyber threats will become increasingly insufficient. Intelligence and information sharing enable organizations to improve situational awareness pertaining to the threat landscape, and provide security professionals with stronger opportunities for prevention of threats.

- **Implement the best tools and methodologies for preventing cyber crime.** Obtain a multi-level security architecture that defends enterprise cloud, network and mobile devices. Implement segmentation and segregation for networks and functions. Keep operating systems and software up-to-date. Work with a reputable vendor that can tailor solutions to your organization's unique needs. The right security tools play a huge role in stopping organized cyber crime.

- **Follow industry best practices.** For example, those associated with GDPR, NIST recommendations, HIPAA and PCI-DSS.

- **Build partnerships across both public and private organizations.** Strategic alliances are vital when it comes to driving successful security programs, as coordinated cross-organizational activities can dilute or disrupt threat actors' plans.

- **After experiencing a cyber attack, investigate thoroughly and consider engaging appropriate authorities.** While authorities often lack the resources to pursue every case, reporting can help authorities track cases attributed to organized crime groups, potentially contributing to takedown efforts.

For enterprises that want to avoid digital damage caused by organized cyber crime, understanding trends and tactics is critical. Let's put organized cyber criminals out of business.

Learn more about preventing organized cyber crime here or find more information on CyberTalk.org.

3 What is Magecart? How this Hackers Group Steals Payment Card Data, CSO Online, David Strom, December 23, 2021
4 Notorious Cyber Crime Gang Behind Global Bank Hacking Spree Returns with New Attacks, ZDNet.com, Danny Palmer, August 30, 2018