CYBER SECURITY PRIMER

UNDERSTANDING THE STORY & INDUSTRY CHALLENGES

About Us

CTM360® is a subscription service offering 24 x 7 x 365 Cyber Threat Management for detecting and responding to cyber threats. Headquartered in the Kingdom of Bahrain, CTM360 specializes in offensive defense - a mentality that looks to neutralize and eliminate threats in infancy - and strives to strengthen a subscribed member's security posture by making them a smaller target. CTM360 currently caters to 25 of the Top 50 Banks across the GCC, as well as entities in Oil & Gas, Healthcare, Sovereign Wealth Funds, Aviation and other sectors.

Offered as a service and with an ecosystem built in the cloud, CTM360 remains a leading detection & response provider in cyberspace and for the digital domain. Noteworthy statistics include 58,000+ unique incidents managed, 4.5 billion hacked accounts indexed, 30,000+ digital assets inventoried and 300 executives protected. CTM360 specializes in threat hunting and neutralizing in cyberspace, digital risk management, threat intelligence, corporate & VIP brand protection, anti-phishing and more. For more information, visit http://www.ctm360.com

CTM360®

I. Threat Landscape

Cyber threats are evolving in variation & sophistication at an exponential rate

The variation and sophistication of cyber threats is directly proportional to the rapid growth and penetration of the internet. What we are witnessing today is just the tip of iceberg given the exponential growth of social media and the ‘Internet of Things’ (IOT).

The broader category of cyber threats, i.e. cybercrime, Hacktivism, cyber wars and cyber espionage are all on the rise. For cybercrime, was year is predicted to be dominated by ransomware, followed closely by Financial Frauds and Advance Fee Frauds. Hacktivism and cyber espionage, which heavily leverage APT techniques, malvertised apps, jail-breaking of cloud applications, doxing, ghostware and sextortion will also be a part of everyday hacking news. It is also expected that more newly-coined terminologies will represent what are currently unknown attack techniques and campaigns.

Commentary of the cyber threat landscape is altogether incomplete without the mention of the Deep Web, DarkNet, Tor and Bitcoins. The explosion of the Tor user community and enhancement in ease of usage is facilitating entry of new threat actors, whereas bitcoins has become the currency of choice for cyber criminals; the Deep Web and DarkNet also remain under-the-surface and an ever-growing incubator of cyber threats – both remain rich cultivating grounds for the next big cybersecurity incident.

II. Social Engineering

Humans are the weakest link in Cybersecurity

Almost all cyber-attacks rely on social engineering of at least one of the attack stages; yet, today this aspect gets the least attention. Social engineering uses manipulation, influence and deception to get a person, typically a trusted insider within an organization, to comply with a request. The request is often to release information or to perform an action that will, unknown to the person, be beneficial to an attacker. Kevin Mitnick, the world-renowned hacker / converted Security Consultant, has written a book on how he aggressively used social engineering to breach the most difficult stages of his hacks - who needs to break a lock when someone will willingly open the door for him?

Social engineering attacks are getting more sophisticated as social media provides ample reconnaissance information to reinforce the attack. To us, it is a straightforward conclusion that the proportion of time, effort and investment on making the staff more vigilant needs to increase.

III. Cyber Kill Chain

Containment of cyber threats in the early stages is not getting the right attention

'The importance of detection and response is in the first 3 stages of the Cyber Kill Chain'

A concept initiated by Lockheed Martin to understand different stages of a cyber-threat, following the trails of the Cyber Kill Chain makes logical sense and leads to effective incident response. What the CTM360 team has realized is that in current industry practice, there is often more focus and investment on the last 4 stages of the kill chain. Detection, disruption and destruction of an attack in those stages is no doubt very important; however, we place higher emphasis on addressing incidents at the early stages of Reconnaissance, Weaponization and Initial Delivery.

For example, an IT or Security vendor staff touting details of your infrastructure on his Linkedin profile is definitely making the Reconnaissance stage effortless. Organizations need to be wary of such casual revelations. Another example is that of cousin domains, which are set up for sending out impersonated emails – these should be disrupted at an early stage.

IV. The Future

Dynamics of managing information security vis-à-vis cybersecurity are different

"Why Cybersecurity will split away from Information Security'
Let us view the past to better understand the future. Over twenty years back, most organizations had no Information Security functions or personnel. From then onwards, with connectivity to the internet, organizations started having the function of IT Security reporting to the Head of IT. Then, approximately 15 years ago IT security managers started getting the titles of Information Security Manager, yet they still reported to the Head of IT. Over the last 10 years, the CISO role has matured and has split from IT, mostly reporting now to the CRO or CEO. This was done to split the Security Governance from Implementations of Controls whereas the latter is rightly still remains under IT.

Very soon, we anticipate another upcoming transformation – the security industry will likely split Cybersecurity from Information Security. There are many reasons for this: Firstly, cybersecurity is all about the external attacks, i.e. cybercrime, cyber espionage, Hacktivism, etc., whereas Information Security is more inward-looking and standards-based. Secondly, cybersecurity requires highly-focused Detection and Response capabilities to handle external attacks. Thirdly, the mode of operations in a cybersecurity team mimics the actions of a country’s defense forces and often, finely-tuned internal security / intelligence agencies. This is the crucial reality of the world we live; to remain relevant, it is imperative that traditional Information Security is balanced with the ever-evolving dynamics of Cybersecurity.

V. Offensive Defense

"If the gap between cyber attacks and the security industry is widening, a drastic paradigm shift is needed"

With the cyber security industry spend projected to grow to $2 trillion by 2019, tremendous growth potential is claimed in the new technologies or services launched by different vendors; however, despite this spend, it is also projected that the gap between cyber attacks and the security industry will continue to widen for the foreseeable future. Clearly something is wrong. Should we continue down this path, the security industry will always chase threats and not ever be in a position to thrive in the threat landscape.

The wider community needs to focus on re-aligning how it views and counters cyber threats. Currently, waiting for threats to impact the perimeter and then pursuing remediation is standard – this is too late.

Coupled with the belief that stopping the attacks early in the cyber kill chain is vital, an offensive defense perspective not only empowers but also strengthens organizations. Offensive defense is an approach of invading an attacker's territory and limiting the time and space he has to construct an attack. This is starkly different from counter-hacking or offensive hacking.

"Why Offense Defense?"

Offensive Defense is a highly effective way to tackle threats before they impact the perimeter of an organization. With agility in mind, incident response in cyberspace (i.e. cyber neutralizing) can preempt any attack before it becomes a major problem.

Extending this to digital risk management, an organization's overall posture will be strengthened once a company adopts an agile and determined mind-set. Instead of passively waiting for attacks to happen, any organization can look to stop incidents before they become pervasive threats.