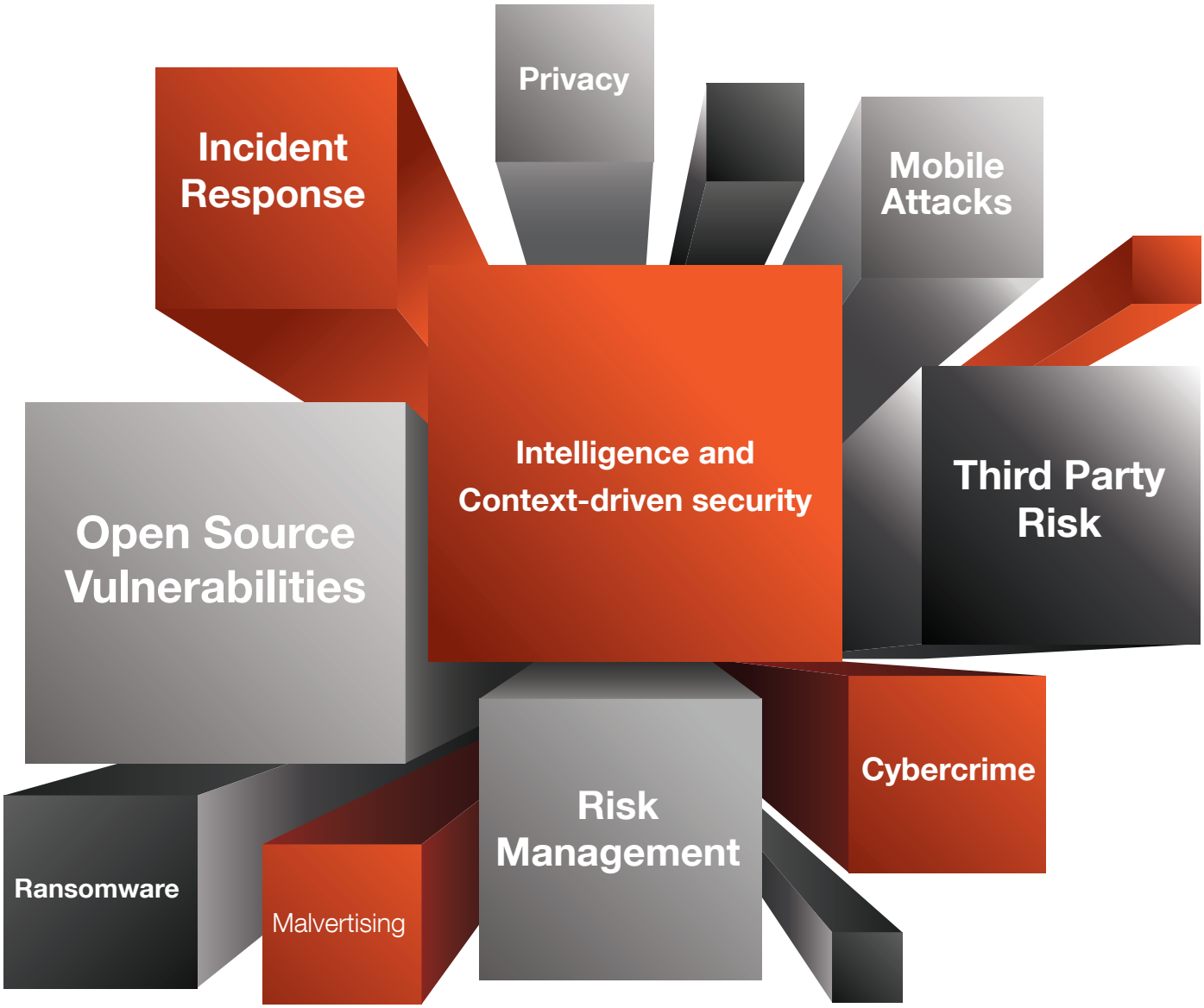
CISO CYBERSECURITY

PERSPECTIVES

Felix Mohan,
CEO, CISO Cybersecurity

2015



PERSPECTIVES 2015

Cybercrime

If 2014 was the year of the breach – it was courtesy cybercriminals and their cybercrime industry in full throttle ably supported by the complacency of victim organizations. With more high value assets projected to migrate into the cloud and online, criminals will find more attractive targets in 2015 to go after. But as law enforcement gets more effective with take-down of criminal activities and increased arrests, criminals will increasingly operate from within the deep web using darknet services like Tor for communicating with their C&C infrastructure (we witnessed the Reveton ransomware use Tor). Given the buyers' concerns on getting caught by law enforcement, cybercriminal gangs are offering anonymity and untraceability in their wares at a premium. Also, with the high profile breaches of 2014, there is a glut in the underground marketplace for credit cards, and their prices have crashed. Compared to credit cards medical record data is selling at about 15x times, and therefore breaching hospitals for harvesting medical records will see an upswing. 2015 will also see far greater collaboration between cybercriminal gangs as they pool their individual strengths to breach entities that are getting progressively better protected. But the criminals will continue to compete in the market place to sell their stolen wares.

Incident Response

The high profile breaches of 2014, that included JP Morgan Chase (with an annual security budget of $200 million and over 1000 top notch security professionals in-house), there is greater consciousness about the ineffectiveness of technical controls and the need to accept the reality of operating their businesses in a compromised state. In this state, detection, response and recovery become important and 2015 will see many organizations turn their attention to identifying Indicators of Compromise and implementing Enterprise Incident Response Plans. Increasing numbers of organizations will build in-house capability or retain on-demand service for recovering evidence, conducting root cause analysis of the incident (not just the symptoms) and conducting forensic investigation.

Intelligence and Context-driven security

2014 breaches have underlined the ineffectiveness of technical controls to prevent intrusions. Obtaining situational awareness of the environment in real or near-time is becoming crucial to mitigate risks. Both Target and JP Morgan Chase attacks could have been thwarted in the early stages if network anomalies and user activities were picked up, for instance when the attackers were querying the AD to map out the network layout and inventory. In 2015, with lessons of the 2014 breaches in hindsight, organizations will start to baseline their networks and systems to know what are normal.

2015 will see organizations turning to security intelligence platforms that integrate information from events and packet flows with contextual data to provide better detection and vulnerability prioritization. Also there will be greater interaction between silos of technical controls, for instance between SAST, DAST and WAF. Organizations will begin to ask for interoperability as a criterion for buying technical controls. External security intelligence feeds into the organization will start to get customized and be provided as intelligence-as-a-service by vendors. Such service will become a big market in the next 3-4 years.

There will be more adoption of big data platforms linked to the security intelligence platform to acquire insights from the security event and flow data. Better security insights will become crucial to combat APTs and targeted attacks.

PERSPECTIVES 2015

Risk Management

Risk management will become more threat-centric and will be supported by formal threat modeling techniques like STRIDE and DREAD. Risk management will underscore the fact that it is not possible to have a 100 percent secured environment. In 2015 organizations will shift from the check-in-the-box risk management to actually analyzing their risk appetite, and identifying what the business relies on most (the crown jewels) and invest efforts and cost on their protection and recovery. Organizations will increasingly adopt cyber insurance as a means of transferring risks.

Privacy

With the latest addition of Sony to the string of PII breaches, privacy has become a hot topic. The victims' huge business costs due to reputational damage and loss of customer trust and churn, has forced a greater focus on protecting PII as both a compliance and business risk issue. Governments will evolve the scope and content of data privacy rules and in 2015, many countries including EU, India, Australia, Japan, S Korea, Canada, countries in Latin America and many others may enact more stringent data privacy laws and regulations.

Third party risk

With the inexorable shift to cloud there will be increasing loss of ownership on organizational infrastructure. Loss of ownership would translate to diminished control and organizations will become dependent on the diligence of third party security processes. However, going by the trend of breaches, many of them have been mounted via third parties and partners. Therefore, organizations will put in stringent security requirements in their third party contracts along with stiff liabilities for attacks whose origins are attributed to the third party.

Mobile attacks

Mobile attacks will grow rapidly and will reach an unprecedented threshold. A major contributor to this state of affairs will be Android OS fragmentation (most users are stuck in outdated versions of Android that are full of security holes - just about 3% of Android devices in use are on the latest versions, while over 33% users are still on Gingerbread that was last updated in Sept 2011).

There will be many new mobile malware generation and exploit kits available in the wild that will make it easy for cybercriminals to target mobile users. Their task will be made easier because most users either don't want to or can't update their systems and software with the latest patches. Mobile phishing will become common to divert users to malicious sites and mobile App Stores will continue to be the major source of malware with increased use of compromised advertising networks to serve malicious advertisements (malvertisements) that direct the mobile user to malicious apps in the App Stores.

On average organizations would release an app every 6-8 weeks. This does not provide adequate time for thorough app testing, and most apps would be released and function in a perpetual beta state. Given this reality, 2015 will see organizations putting in clauses for "maximum time to recover/correct a bug" in their mobile app development outsourcing contracts, with stiff liabilities in event of non-compliance.

Apple iOS platform saw a new era of threat in Nov 2014 with the WireLurker malware that compromised even 'non-jail broken' devices. This significantly diminished the confidence of users in the security assurance of the Apple platform. 2015 will see bigger Apple breaches.

At the network layer, fake femtocells and GSM base station attacks will rise, so will the man-in-middle attacks due to compromised WiFi networks with increased usage of mobile data offloading options.

Ransomware

With Cryptolocker, ransomware got firmly entrenched as a lucrative attack vector for criminals. Now it is making an entry into mobile devices as was witnessed in the Reveton malware for Android. The sophistication of the ransomware has increased with their usage of Tor network for hiding its communication with its C&C servers.

2015 will see ransomware going after data backups in the cloud, by first compromising end user devices to steal their cloud login credentials and then encrypting the user's data in the cloud before demanding ransom. This would leave the user with no backup, and make the demand for ransom much more effective for the criminals.

Criminals will target organizations in addition to individual users. In compromised organization networks the malware will search for high value targets such as network storage and encrypt those to demand higher ransom.

Malvertising

2015 will see a rapid rise in the volumes of malvertisements delivered through compromised ad servers that are tricked to serve advertisements containing malicious codes or direct unwary users to malicious sites. Cybercriminals will prefer to exploit this vector because it is not possible to block or test every ad network (most of which are legitimate). They have the advantage because reputed websites (news and infotainment) are hardly ever blocked by office firewalls. Also convenient for them is the ease with which they can get access to millions of users with minimal effort – all they have to do is write the malvertisements code and leave it to the ad networks to do the dirty job.

PERSPECTIVES 2015

Open Source Vulnerabilities

The first taste of blood was had with Heartbleed, followed by Shellshock and POODLE. Vulnerabilities that lay hidden and dormant for many years suddenly rose to haunt and be exploited by attackers. What the world learnt was that core Internet protocols weren't infallible and that there are significant portions of insecure code in computer systems in widespread use. And now there is no looking back - 2015 will see more vulnerabilities tumbling out of the closet as criminals resort to detailed code analysis and fuzzing to search for new holes in open source protocols to exploit.

Felix Mohan,
CEO, CISO Cybersecurity

CISO CYBERSECURITY
www.cisocybersecurity.com