Cybersecurity essentials for capital markets firms in the digital age

wipro

Global IT spending is projected to rise to $3.7 T in 2018, growing by 6.2% from 2017, while the information security market is projected to grow 8.7% to $124B in 2019 and is expected to reach $170B in 2022.[1] The growth of security solutions is outpacing IT spend globally due to the rapid proliferation of digital, increasing regulations on security, risk and data privacy, and the growing volume of cyber threats. There has been a surge in the number of threat vectors and vulnerabilities in enterprise networks, thereby increasing cybersecurity risk exponentially. Based on a recent study[2] the cost of cybercrime is estimated to be in excess of $600B. Financial institutions including securities and capital markets firms are not immune to this risk given their increasing reliance on information technology, growth in mobile/digital channels, and accelerating pace of electronification of global markets. The risk and exposure can be multi-fold: direct operational and financial impact due to damage caused by successful cyberattacks or indirect impact due to reputational risks and financial penalties from regulators who are increasingly adding to the infrastructure and compliance requirements around cybersecurity. The EU GDPR (Global Data Protection Regulation) regulations which went into effect in May, can result in fines up to €20M if organizations fail to report a cyber-attack within 72 hours.

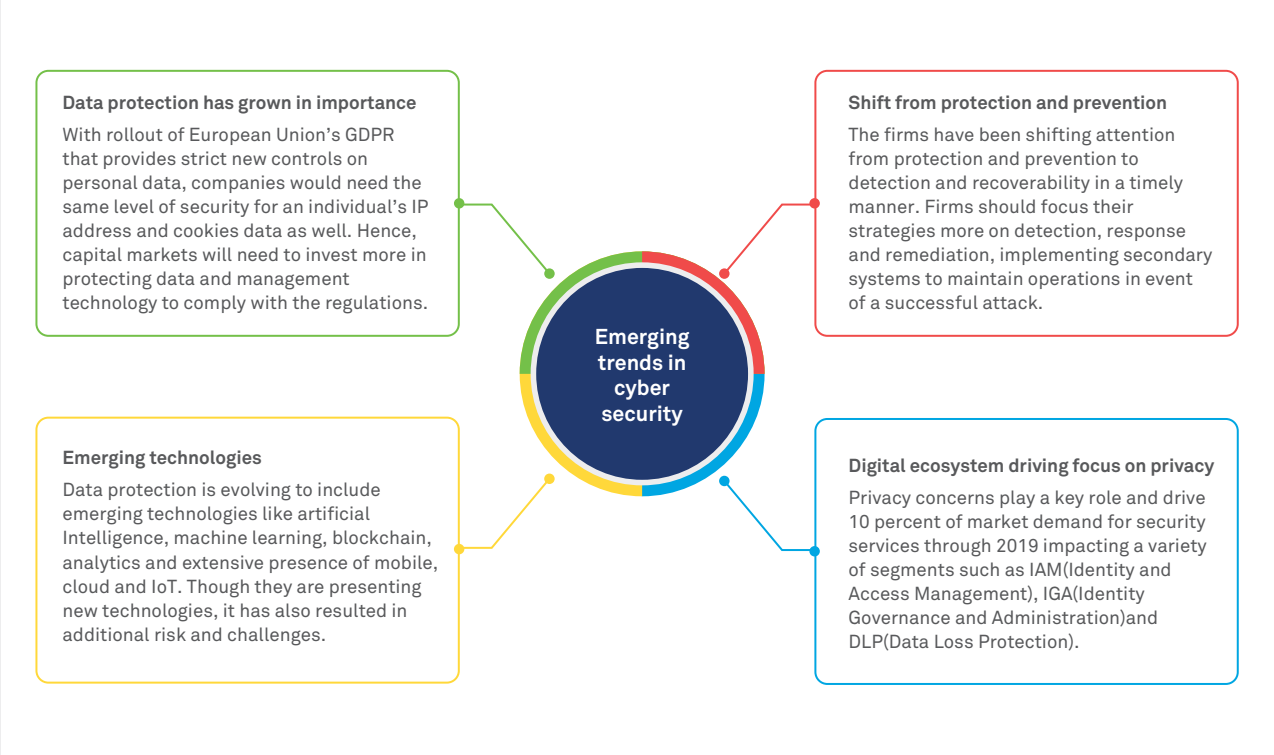

Figure 1: Emerging Cybersecurity Trends

Types of cybersecurity threats

Global companies spent up to 26 percent more for cybersecurity in 2018, as the average cost of a data breach is now up to USD 1.23 million for large companies (up 24 percent from 2017)[3]. Financial firms have the second highest cost per capita for data breaches while healthcare tops the list[4]. The frequency, sophistication and impact of cyber threats are at an all-time high. The top cybersecurity threats in 2018[5] are shown below.

Today, 99% of computers are vulnerable to cyber-attacks, 68% of funds lost as a result of a cyber-attack were declared unrecoverable.

Figure 2: Types of Cybersecurity Attacks

Impact of cyber threats on capital markets

According to a study published by the International Organization of Securities Commissions (IOSCO) research department and the World Federation of Exchanges office, around half of the world's securities exchanges were the subject of cyber attacks last year.

Cyber threats in capital markets may lead to manipulation of order management systems leading to incorrect feeds, false orders/ non-submissions, and corruption of trade surveillance systems thus enabling manipulative, illegal and abusive trade practices.

All this can result in triggering automated rogue trading strategies, thereby increasing the chance of flash crashes. The cybersecurity landscape for asset and wealth management firms is also fraught with an array of threats aimed at stealing or compromising clients' investment or personal data. With the growing adoption of wealth management applications on mobile and via cloud-based services, attacks like DDOS, ransomware and phishing are gaining popularity.

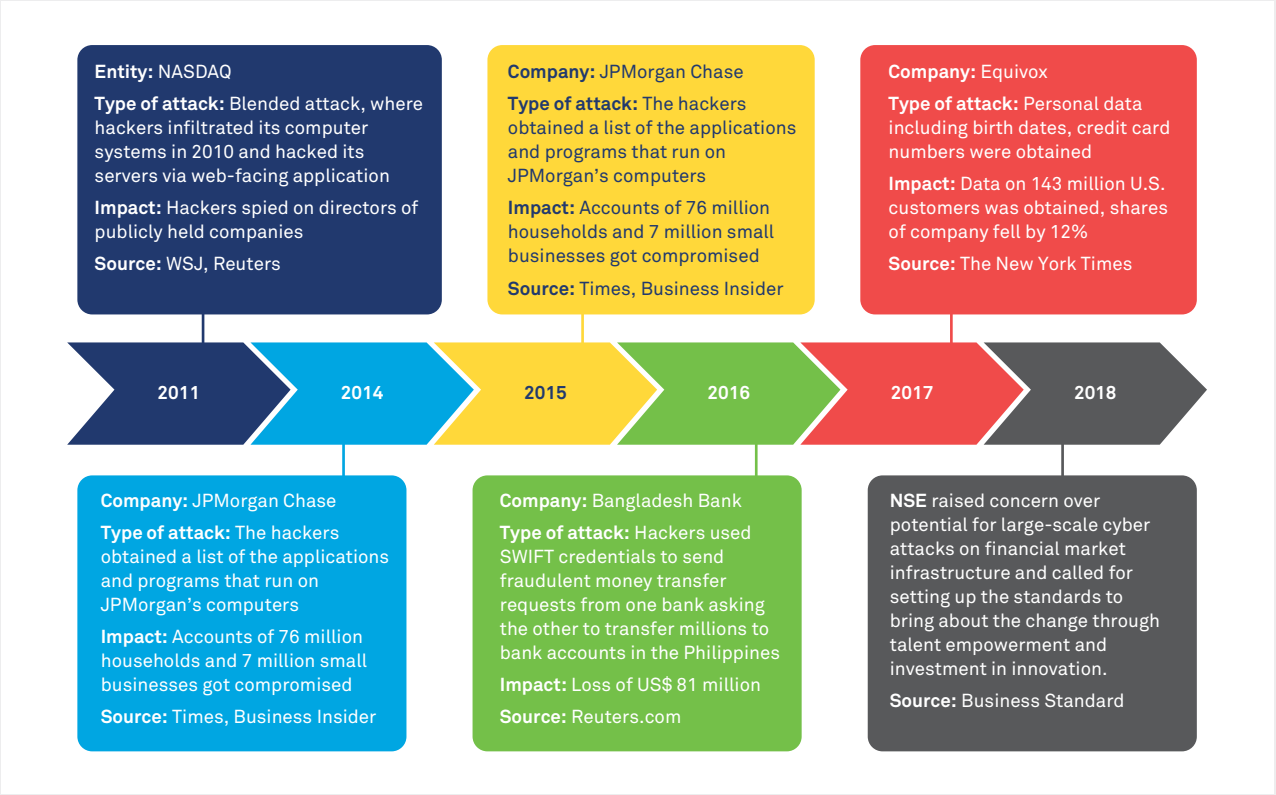

Figure 3: Top cybersecurity threats

Essential cybersecurity measures

Cybersecurity leaders should seek the right balance between risk, usability, resilience, and price. However, it is predicted that by 2020, more than 60% of organizations[6] will invest in multiple data security tools like data loss prevention, encryption, unified threat management, intrusion detection systems, etc., up from 35% today.

Figure 4: Cybersecurity tools/ solutions

CISOs at capital markets firms will need to improve their security posture by taking several key and essential measures that are part of an integrated approach to cybersecurity

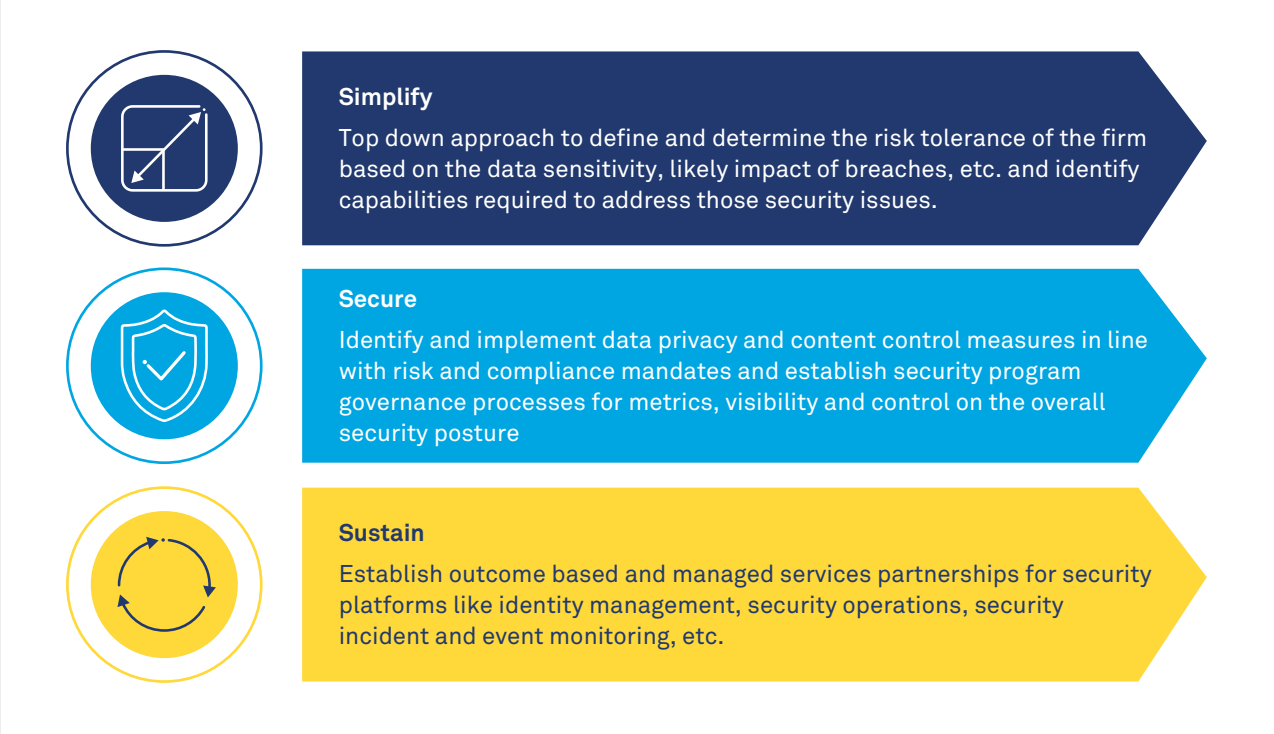

Figure 5: Integrated 3S approach

Capital markets institutions worldwide are driving innovation in cybersecurity by combining in-house expertise with specialized capabilities around security, governance, risk and compliance.

Figure 6: Case in point

Platform-based approach to manage cybersecurity

Managing cybersecurity in the digital age requires a vastly different blueprint to traditional methods of managing security. The imperative is to create a multi-disciplinary approach that combines risk and compliance, IT, and security capabilities and deliver platforms that address the broad security needs of an organization. The security platforms typically cover a gamut of solutions that span across core security domains, operations, audit/ review, and AI/ analytics. The advantage of the platform-based approach is the ability to bring deep specialization in each of these fundamental building blocks to cybersecurity along with the standardization and benchmarking of policies and procedures.

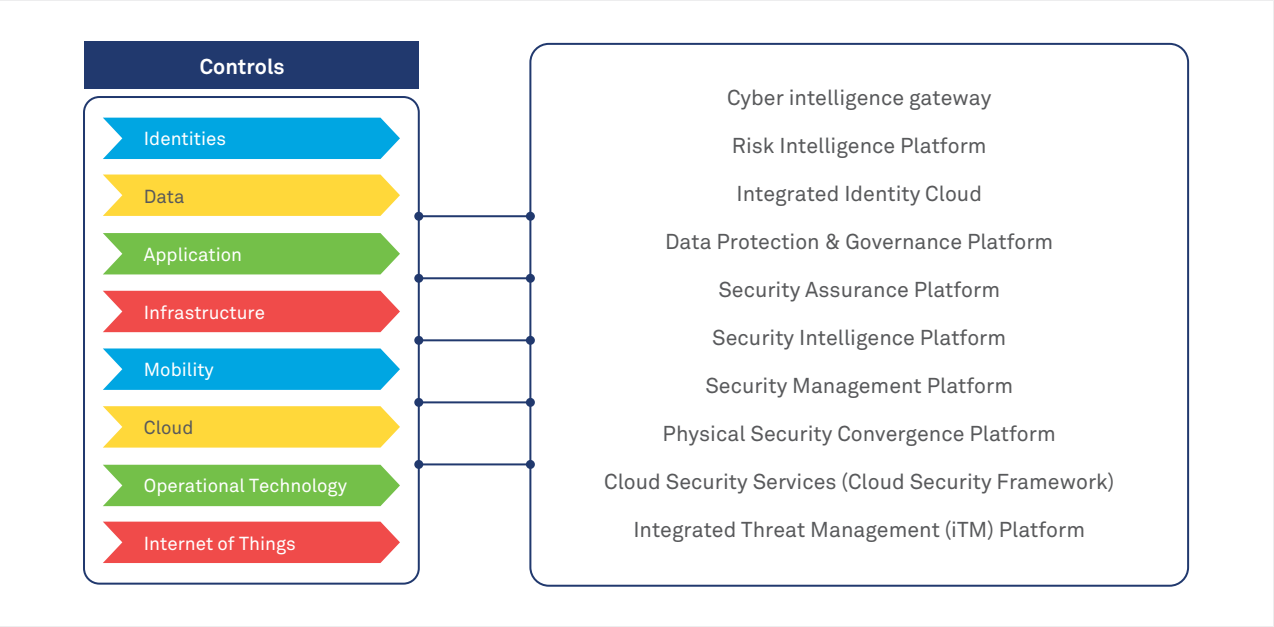

Figure 7: Cyber Security Platforms

New ways of working to prevent cyber threats

Cyber threats are growing in frequency and severity, thereby making traditional approaches to security less effective. Along with increased focus on fundamental aspects like updating patch management and stronger third-party risk and compliance procedures, emerging technologies like Cloud, AI and ML, RPA, and Big Data can help orchestrate more effective cybersecurity strategies.

The use of sequential hashing and cryptography in **Blockchain** systems, along with decentralized structure has made it impossible for a party to alter any data on the ledger, thus protecting client data and trade information and making it nearly impossible for hackers to attack.

AI and Machine Learning (ML) algorithms help in fast detection of threats and limiting their spread by identifying outliers from normal patterns. They also help in keeping pace with the continuously changing threat landscape by training algorithms on new trends.

RPA helps in lowering security-related efforts associated with employee training on security policies and practices as it provides a zero-touch environment. Tools and solutions come with audit logs that provide an immutable trail on the usage of PII information, which is required for regulatory reporting and compliance purposes.

Cloud is reaching an appreciable maturity level. Firms should proactively address the risks associated with cloud computing and map regulatory requirements with their cloud approach to ensure resilience, availability and disaster recovery capabilities. Cloud-based security solutions complement the on-prem solutions with low maintenance costs, high availability and advanced analytics.

Big Data is being used to identify cyber-attack trends from the vast amount of security data mined across end point devices. One of the growing technologies in the field of analytics is UEBA (User and Entity Behavior Analytics) which takes note of the normal conduct of users and detects deviations from normal patterns using machine learning, algorithms and statistical analyses.

References

[1]https://www.gartner.com/newsroom/id/3871063

[2]https://www.csis.org/analysis/economic-impact-cybercrime

[3]http://business-review.eu/tech/it/kaspersky-lab-survey-companies-around-the-world-spending-up-to-26-pct-more-for-cyber security-in-2018-171287

[4]Forrester Top Cyber Security Threats in 2018

[5]IBM Security and Ponemon Institute Cost of Data Breach Study 2018

[6]https://www.gartner.com/newsroom/id/3836563

About the author

Sakshi Agarwal
Pre-Sales Consultant, Financial Services
Securities & Capital Markets,
Wipro Limited.

Sakshi is working in Wipro as a Pre-Sales consultant for Securities and Capital Market clients across the Americas and Europe.

She has completed her Master's in Business Administration from IIM Udaipur, batch of 2016-18.

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035,
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 175,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**

IND/B&T/JAN2019-JUN2019