CONTRIBUTORS

- **Justin Doebele**
  Executive Director - Content
  Forbes Asia
- **Sean Duca**
  Vice President, Regional Chief Security Officer
  Palo Alto Networks
- **Anil Bhasin**
  Managing Director - India & SAARC
  Palo Alto Networks
- **Rama Vedashree**
  Chief Executive Officer
  Data Security Council of India
- **Mandar Marulkar**
  Chief Digital Officer
  KPIT Technologies
- **Ramachandra Hedge**
  Vice President, Chief Information
  Security Officer
  GENPACT
- **Eric Anklesaria**
  Vice President & Global Leader
  Banking & Capital Markets Transformation
  Capgemini
- **Sameer Ratolikar**
  Executive Vice President & Chief Information
  Security Officer
  HDFC Bank
- **Prof. S. Sadagopan**
  Director
  Indian Institute of Information Technology,
  Bangalore (IIIT- B)
- **Sridhar Govardhan**
  Chief Information Security Officer
  Wipro
- **Saritha Auti**
  Chief Information Security Officer,
  Assistant Vice President Cyber security
  Cognizant
- **Shree Parthasarathy**
  Chief Innovation Officer
  National Leader - Cyber Risk Services
  Deloitte India
- **Hitesh Mulani**
  Group Chief Information Security Officer &
  Vice President - IT Partner Collaboration &
  Process Excellence
  Mahindra & Mahindra

NAVIGATING THE DIGITAL AGE | INDIA EDITION

SecurityRoundtable.org

paloalto NETWORKS® | Forbes Asia

NAVIGATING THE DIGITAL AGE

THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS

INDIA EDITION

Supported By

DSCI
PROMOTING DATA PROTECTION

NAVIGATING THE DIGITAL AGE

THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS

INDIA

In partnership with

Forbes Asia

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers - India

Printing and Binding: Spenta Multimedia Pvt Ltd

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers
In partnership with:
Forbes Media Asia Pte Ltd
501 Orchard Road
#08-02 Wheelock Place
Singapore 238880

Cover illustration by Tim Heraldo

DISCLAIMER

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers (the Guide) contains summary information about legal and regulatory aspects of cybersecurity governance and is current as of the date of its initial publication (February 2019). Although the Guide may be revised and updated at some time in the future, the publishers and authors do not have a duty to update the information contained in the Guide, and will not be liable for any failure to update such information. The publishers and authors make no representation as to the completeness or accuracy of any information contained in the Guide.

This guide is written as a general guide only. It should not be relied upon as a substitute for specific professional advice. Professional advice should always be sought before taking any action based on the information provided. Every effort has been made to ensure that the information in this guide is correct at the time of publication. The views expressed in this guide are those of the authors. The publishers and authors do not accept responsibility for any errors or omissions contained herein. It is your responsibility to verify any information contained in the Guide before relying upon it.

Introduction

Forbes Asia – Justin Doebele, Executive Director - Content

As more and more of our daily lives and work are based in cyberspace, the potential risks and damage that can be caused by hackers also rises. The need for cybersecurity therefore also becomes paramount in this environment. One major example of this is the recent controversy that has been swirling around potential Russian meddling in the recent U.S. elections, which may have involved sophisticated electronic intrusions. Thus, the stakes have been higher, and the opportunities never better, for those in the cybersecurity industry. Demand for services in this sector can really go in only one direction—growth and more growth. Add into this mix multiple disruptive technologies that are emerging, such as blockchain, IoT and SaaS, and the threat levels become even more complex. Perhaps the biggest of these developments is AI, a powerful technology that can be used for good or ill.

The importance of cybersecurity among the leading companies has now become a priority in the C-suites, and it is being recognized within the various dimensions important for an enterprise, such as brand value, corporate reputation, customer satisfaction and loyalty—not to mention the monetary impact that result after a major breach in legal costs. As the old saying goes, an ounce of prevention is worth a pound of cure.

Achieving the right balance is never easy, and very much a moving target, between having an organization that is open and flexible, and yet secure and safe. For example, many financial services firms, which have security as a core paradigm, would also like to improve their competitive advantage by partnering with fintech start-ups, which by default may have different security standards. Thus finding the right combination of giving your corporate community, be they clients, suppliers or partners, access to networks and databases, while still providing the appropriate levels of security, all while operating in a dynamic and fast-changing environment of evolving technologies and threats, can be a daunting challenge.

There's no doubt that threats are not just external, as corporate leaders are required to make worst-case scenarios regarding their own internal networks and their

own human resources. Sadly, cyberattacks can originate just as easily from inside an organization as well as coming from outside—some being opportunistic when a flaw is unintentionally created or exposed.

Thus the need for vigilance is a never-ending one. Organizations that build in an awareness of the risks, which create environments in which security becomes a given and not just a bolt-on, will naturally have a better competitive advantage. Leaders must learn to define the challenge in a way that this awareness takes root across an entire organization. It may not be the most exciting of tasks, and will by its nature be one that goes on mostly out of the spotlight. The best security is often the kind that gets the least awareness, as the time when it attracts the most attention is when it fails.

Gathered in these pages are a host of experts who have developed a recognized status in the area of thought leadership in cybersecurity. They can help to provide guidance and pragmatic wisdom of how to adapt and develop a strategic approach that meet the various goals need to be successful but also safe and secure.

Foreword: The Importance of Cybersecurity for Executives in India

Palo Alto Networks - Sean Duca, Vice President, Regional Chief Security Officer

As we live in an increasingly interconnected era, leveraging new technologies and transforming the way we do business, we need to raise awareness of security concerns and act to reduce the risk rather than avoid it. It's simply about being sensible and trying to stay ahead of cybercriminals by understanding current and potential threats, and what can be done to mitigate these risks.

Cyber risk is a serious challenge and should be treated as a business issue rather than a technology issue. No data breach should come as a complete surprise; rather, as a foreseeable event for which you are completely prepared. Yet for years, every time a new security challenge impacted an organisation, this forced it to spend valuable capital on cybersecurity products that focus on narrow cyber risks or the specific 'threat-du-jour'. The company's IT staff cobbles together products and services from various legacy vendors with little strategic planning or thought about the core business risks. They then hope that their mountain of legacy technology is updated often enough to provide some defence against the fear and uncertainty being spread about cyberthreats in daily news headlines.

What is evident, however, is that this approach to cybersecurity isn't working. With the number and severity of breaches on the rise around the world, what may seem like fear-mongering is in fact a new reality: the falling price of computing power has allowed cybercriminals to launch low-cost, low-risk attacks yielding high returns. Hacker toolkits — easy-to-use, highly effective malware that's growing in popularity — enable novices with minimal technical knowledge to understand your digital environment better than you do and breach your increasingly expensive and complex legacy cyber defences.

The traditional answer to these challenges - adding more legacy technologies one on top of another – actually creates a new layer to the problem. Point products work in their own respective silos and were never designed to interoperate or share information with each other. While more products may seem to be getting you closer to solving the problem, they are in fact creating unnecessary complexity.

With the rise in successful cyberattacks, cybersecurity is becoming an increasingly strategic concern that threatens the foundations of enterprise value for business leaders in India as well as the wider Asia-Pacific region. As India pushes ahead with its "Digital India" initiative, which aims to ensure Government services are made available to citizens electronically, it also means that the country is at a high risk of facing cyberattacks on its infrastructure. The subsequent impact on private entities is, unfortunately, inevitable.

No leader wants his or her organisation to be splashed on the front page of a newspaper due to a cybersecurity breach that hurts its reputation and profitability and undermines its business model, but this is the reality we face today. Cyber incident preparation is actually about prevention—preventing your business from going downhill. And that's a message that should be conveyed from the very top of the organisation across business lines and functions, from the back office to the front office. In Palo Alto Networks State of Cybersecurity Survey APAC, the three foremost cybersecurity challenges organisations in India faced in 2017 were employees' lack of cybersecurity awareness (47%), risk from third-party services (43%) and migration to cloud (35%). With leadership-mandated initiatives to practice good cyber hygiene across the business, all of these concerns can be tackled.

In light of how businesses are evolving, our approach to solving security challenges needs to evolve as well. We need to look at how these manual processes can be automated and move beyond technical point product solutions, towards deploying defences to protect what is of most value to companies (and attackers). By increasing the speed and automation of our defences, we can slow down and potentially deter the adversaries by reducing their success rate.

How then can you forestall and thwart an attack?

Lessons from abroad

Many companies—particularly those in India—believe that their current strategies around the technologies they have deployed, the teams of people they have to manage and operate them, and the processes they use aren't perfect, but seem as if they are good enough; and many companies are confident that any problem will right itself eventually. Some may even believe that a major breach could never happen to them, impacting only large enterprises, the government, or companies in the United States and Europe. However, history—and the range of stolen data—has shown that any company, irrespective of size and location, is vulnerable.

Breaches tend to hit the news only when someone outside the organisation discovers and exposes them. What may be contributing to this perception of many countries, including India and across Asia Pacific with no mandatory data breach disclosure laws. Because no regulation in India today forces public disclosure of data breaches— and the public discussion that usually follows disclosure—companies, consumers, and regulators may underestimate the full scope of the threat and damage. Though no regulation is a panacea, organisations in India, and elsewhere in Asia-Pacific, do not need to reinvent the wheel: rather, they can look to other continents that have dealt with these pressing issues before and answered them in the context of regulation. These countries, such as the United States and some in the European Union, have multiple data breach notification laws and have explored mandatory data breach reporting and notification when personal data is compromised.

So how should companies in Asia-Pacific approach instituting a security approach that is up to par with global standards? Not

all lessons from abroad are mandates. For this reason, the National Institute of Standards and Technology (NIST) Cybersecurity Framework was developed in an open, collaborative partnership in the United States between NIST, a US Government agency, and the private sector. This framework helps guide executive management and boards of directors; points to globally accepted, industry-driven standards for risk management; and provides a common language and benchmarks for cyber resilience across an organisation (from boardroom to IT analyst), when dealing with stakeholders and third parties, or when operating across borders.

Regardless of how executives and boards structure their strategies for managing cybersecurity risk, they should not just be lists with technology check boxes, but rather solution agnostic and interoperable among different systems.

Three investments to mitigating risk

There is no doubt a focus on cybersecurity provides longevity to a business and can help differentiate it from its competitors — for both good and not-so-good reasons. Strong cybersecurity is fundamental to the growth and prosperity of all organisations in the public and private sector; to make India's online systems and networks more resilient; and to provide trust and confidence to its citizens, businesses, and customers.

To that end, we need to look at how we can become efficient with our security efforts. Instead of chasing after the elusive silver bullet security product, organisations in India should target investment in three areas to reduce their cybersecurity risk:

1. **Strong cyber defences.**
   Companies should practice good cyber hygiene to protect and maintain their systems and devices appropriately, ensuring they are up to date. This includes a regular backup of data, patching systems and applications, and reducing the attack surface of digital assets as much as possible. By having visibility and taking an inventory of your environment and applications, you can ferret out gaps or deficiencies and note where you lack visibility in your network. Organisations should conduct regular health checks around where and how their data is secured, what applications are in use in their network, who are the users, what do they have access to, as well as the risks and exposures that exist in their organisation.

2. **A well-trained workforce.**
   According to the 2014 IBM Chief Information Security Officer Assessment, human-related errors lead to nearly 95% of all security issues. Companies should therefore educate employees on how to identify and protect their organisations from threats such as phishing, when hackers pretend to be a legitimate entity in an email. Cybercriminals may search online and on social media for an employee's interests and hobbies to craft an attack, in the hopes of luring the worker into opening an infected attachment. Organisations should look to move beyond a compliance check for this training and see how they can invoke change to better defend themselves. Businesses should encourage users to protect their data and their systems at home, as this will naturally flow into the workplace.

3. **Automated platform.**
   With adversaries using automated tools, organisations should seek out automated defence technology that has been built to act seamlessly behind the scenes—part of a platform smart enough to take actions on your behalf, with a minimum of manual effort by your security professionals.

Prevent and respond

In India and beyond, the prevailing perception is that cyberthreats are becoming so advanced that companies can't keep up. The logic goes that if getting compromised is inevitable, efforts should be focused on cleanup after a data breach. Yet isn't an

ounce of prevention worth a pound of the best cure? If we continue to focus on reacting to each security challenge, how have we evolved, and how will that impact our businesses in the future? We need to protect our digital way of life by believing that prevention is possible. This doesn't mean that you must expect to be 100% perfect all the time, but we need to make it fundamentally harder for attackers each time, so they are not successful. With this approach to defence, attackers will need to design and develop unique tools every single time they want to attack an organisation.

For years we believed that simply blocking attacks at 'the front door' to your organisation was enough, but in fact, that's when the clock starts ticking. From that point on, how can you limit your attackers' ability to move around your network and reach their objective—stealing your information, disrupting your services, or undermining the integrity of the data held by your organisation? After gaining entry on one computer, an adversary will look to move around an organisation's network like most users would, ultimately mapping out a route to the servers that store your organisation's crown jewels. Tools will be installed to allow the attackers to remotely control systems from afar. Cybercriminals then hide or encrypt your data before sending the data out of the organisation. So, if all of our efforts are focused on protecting the entry to our organisation, we lose the ability to block the attackers at any stage of the attack lifecycle, allowing the attackers to reach their objective.

However, organisations candevelop prevention controls to disrupt the entire attack lifecycle and prevent a negative material impact from a cyber incident. In order to accomplish the disruption of the attack lifecycle, these are the elements of prevention your organisation needs: threat prevention, threat detection, and threat eradication.

Threat prevention uses known methods to thwart campaigns at each phase of the attack lifecycle. Because of the adversaries' propensity to reuse the playbooks against multiple targets, many organisations are aware of these clues. However, if organisations prevent only known behaviour, they will likely miss an adversary's attacks employing the newest hacking techniques.

Threat detection automatically hunts for clues throughout the enterprise at each phase of the attack lifecycle—it investigates unknown anomalous behaviour wherever it is found and takes the appropriate actions. Detection uncovers attacks that security controls did not initially block, and also brings to light previously unknown malicious activity that organisations must eradicate or minimise.

Threat response blocks future attacks by analysing the new methods and installing additional means to thwart the adversary. In this two-pronged-strategy, organisations must first use newly discovered signs of an attack to protect their networks. Second, they must understand the adversary's objectives to determine what else they can do to prevent the adversary from succeeding.

While similar, all three of these essential tasks are important in their own right, but individually are not sufficient to prevent material damage. With a strong security architecture in place, businesses will be positioned to prevent every threat that is known, discover new and unknown threats as they emerge, and quickly deploy countermeasures to prevent adversaries from reaching their objective.

Each of these tasks should be automated as much as possible. However, this is incredibly difficult to pull off with multiple security solutions that were never designed to work together or share threat intelligence. One way to address is by having security professionals work to make strategic investments across an integrated platform that automatically correlates intelligence collection and the deployment of prevention controls for their organisation.

Conclusion

Like any business risk, cyberthreats are evolving—and so should your organisation's response. Security risk should be a

top concern for executive management and the board of directors in order to protect your business and your customers. Too often, business leaders view security as a matter of compliance and control, which can set up a clash between the needs to protect assets and to foster productivity.

However, cybersecurity can support the goals of senior executives to keep the company running and profitable. Business leaders must set organisational strategy with cybersecurity considerations built into the business planning process. Adopting a framework of standards and accountability will help organisations develop a plan that spells out who is responsible for responding to cyber incidents from a technical, legal, and executive standpoint. Toward that goal, technical and non-technical personnel should all work together to address cyber risk.

The chief information officer (CIO) and chief technology officer (CTO) are always looking for new ways to innovate and differentiate their company in the marketplace. By working closely with the chief security officer (CSO) or chief information security officer (CISO), they can achieve that innovation in a secure manner that mitigates cyber risks. Leaders can also learn from one another. By joining communities such as the Security Roundtable, they can stay up to date with best practices from peers and experts in the cyber arena. The criminal underground shares the latest techniques to launch their attacks, so it only makes sense that we as defenders should share our lessons learned as well. The more we share, the better we can defend ourselves by driving up the cost of a successful cyberattack exponentially.

Armed with the expert insights in this practical guide, organisations can meet this global cybersecurity challenge. Security is a sport best played as a team, and the steps we take now will have a significant and long-lasting impact on the Indian economy now and in the future.

The insights in this guide include advice and best practices from Indian and international thought leaders who are chief executive officers (CEOs), chief innovation officers (CIOs), CISOs, academics and subject matter experts. At the heart of every business should be effective risk management, a thorough understanding of the risks, as well as pragmatic solutions, which include better training and awareness. In cybersecurity knowledge is the key to prevention. And knowledge starts right here.

References:

1. Palo Alto Networks State of Cybersecurity Survey 2017
2. Fortifying for the Future' Insights from the 2014 IBM Chief Information Security Officer Assessment
3. www.securityroundtable.org

Your Cyber Defence has been Breached - What Next?

Palo Alto Networks - Anil Bhasin, Managing Director - India & SAARC

Cyberthreats have quickly risen up the ranks to become the main business threat that enterprises face today. The FICCI – Pinkerton India Risk Survey 2017 ranked 'Information & Cyber Insecurity' as the biggest business risk.

In response, businesses across the board are taking cybersecurity more seriously – Palo Alto Networks The State of Cybersecurity in Asia-Pacific survey revealed that cybersecurity budgets have increased by 92% for Indian organisations in FY 17. This is primarily driven by the growing volume of cyberthreats, its increasing sophistication and the enhancement of existing security frameworks to automated technologies.

As businesses wake up to the seriousness of the threat, cybercrime itself is staying ahead of the game with sophisticated evolutions ranging from malware to cryptomining, leaving businesses increasingly vulnerable. Cybercriminals have the advantage of operating in a decentralised market, which helps them to adapt and innovate faster than cyber defenders, whose effectiveness is shaped by bureaucratic and top-down decision making.

Cyber preparedness, however, is not only about reliance on the internal cybersecurity team or the technology it has at its disposal. The Palo Alto Networks survey also listed employees' lack of cybersecurity awareness (47% of respondents) as the main cybersecurity challenge that organisations face. Without effective employee education, planning and operational understanding in place, businesses in India will continue being extremely vulnerable.

Due to the multiple dimensions they span across, cybersecurity risks should be treated as a business issue. While most enterprises already have a strategy in place to handle different types of crises, including managing the communications process with stakeholders, cybersecurity is an area where many do not do scenario planning, which is critical for understanding the worst cases of potential data breach.

It has now been proven that even the best prepared enterprises as well as governments, are not immune to threat actors looking to steal data or penetrate and disrupt critical systems through various entry points, whether it is the network, applications, the cloud, or even endpoint devices.

As companies no longer operate in isolation and are accountable to their stakeholders, cybersecurity calls for necessary guiding principles in determining how stakeholders are informed about a breach, and how they will be provided with further relevant information as more data is analysed to paint the full picture.

Furthermore, cyber crises are also uniquely challenging - many cybersecurity breaches are discovered by third parties and leaked to the media, with company executives waking up to the news instead of being updated in real time. How companies discover and report breaches takes on tremendous significance as governments across the globe are moving towards a more stringent data and privacy protection regime, as we saw with the European Union's General Data Protection Regulation (GDPR) that came into force in 2018.

While some companies have their own cyber breach response plans, they still need to ask themselves a few questions:

- How well has your plan been tested?
- Has it been workshopped across multiple scenarios?
- Have you run your plan through mock trials?
- Is the plan up-to-date?

Imperative to have a cyber breach response plan

A cyber breach response plan needs to be the blueprint guiding every function in the organisation involved in the response, holding together the precision and speed of the entity's continuous reaction as the breach unfolds. Such a framework should span across cybersecurity, business continuity, reporting, cyber insurance (if covered), reputation management and finally, the legal fallout.

Here are some tips to make your crisis planning more robust and effective:

1. **Stay current and relevant by updating the plan regularly**
   Include input from all key stakeholders and schedule time on the team's calendars to revisit the plan regularly – on a quarterly basis, if possible.

2. **Test the crisis plan**
   Train all employees, including the board, with mock drills. Inject different scenarios into the basic plan and imagine all the different ways in which a breach could impact the business.

3. **Understand your business, down to the day-to-day operations**
   Explore all the machinations of the way your business operates day-to-day. Plan for day-to-day operations with a business continuity plan that is also tested and rehearsed. Additionally, understand what critical systems your business relies on, how they are interconnected, and what their dependencies are. If your response team is busy turning off exposed systems, your business may no longer be in operation.

4. **Be absolutely sure of your continuity plan**
   If your continuity plan is virtually covered in dust, it may also be filled with dated information about old systems and the contact details of response personnel who no longer occupy that position.

There is no silver bullet for cybersecurity. While cybersecurity itself is evolving towards prevention, rather than response, enterprises and governments also realise that every single entity is vulnerable to a cyber breach and are preparing their response strategies.

Such preparation takes time, but is worth investing both the time and effort to build the foundation of how organisations respond to a cyber breach. As cyberattacks continue to grow in volume and complexity, it is absolutely essential to have a robust and tested crisis plan so that your organisation can be well prepared to protect itself in the event of a breach.

TABLE OF CONTENTS

iii INTRODUCTION
Forbes Asia — Justin Doebele, *Executive Director - Content*

v FOREWORD: THE IMPORTANCE OF CYBERSECURITY FOR EXECUTIVES IN INDIA
Palo Alto Networks — Sean Duca, *Vice President, Regional Chief Security Officer*

x YOUR CYBER DEFENCE HAS BEEN BREACHED - WHAT NEXT?
Palo Alto Networks — Anil Bhasin, *Managing Director - India & SAARC*

NAVIGATING THE DIGITAL AGE

2 1. HOW AND WHAT WILL THEY STEAL NEXT?
Capgemini — Eric Anklesaria, *Vice President & Global Leader Banking & Capital Markets Transformation*

6 2. PRIORITISING CYBER RISK FOR THE CYBER SAVVY CEO
Cognizant — Saritha Auti, *Chief Information Security Officer, Assistant Vice President Cyber security*

10 3. HOW DATA GRIDS WILL POWER THE ECONOMY AND INFLUENCE OUR FUTURE
Data Security Council of India — Rama Vedashree, *Chief Executive Officer*

16 4. WINNING THE CYBER-SECURITY WAR REQUIRES A TRULY COLLABORATIVE EFFORT
Deloitte India — Shree Parthasarathy, *Chief Innovation Officer, National Leader - Cyber Risk Services*

20 5. WEAVING SECURITY INTO THE FABRIC OF GLOBAL DIGITAL BUSINESSES
GENPACT — Ramachandra Hedge, *Vice President, Chief Information Security Officer*

26 6. ESSENTIAL BEHAVIOURAL COMPETENCIES TO MANAGE THE NEXT GENERATION CYBER SECURITY RISK
HDFC Bank — Sameer Ratolikar, *Executive Vice President & Chief Information Security Officer*

30 7. CYBERSECURITY - NEED FOR A HOLISTIC VIEW
Indian Institute of Information Technology, Bangalore (IIIT- B) — Prof S Sadagopan, *Director*

34 8. SECURING CYBERSPACE IS KEY TO SUCCESS IN THE DIGITAL AGE
KPIT Technologies — Mandar Marulkar, *Chief Digital Officer*

45 9. INTRICACIES OF OUTSOURCING AND THE IMPACT OF OUTSOURCING ON AN ORGANIZATION'S SECURITY LANDSCAPE AND LIABILITIES IN AN OUTSOURCED SERVICES SCENARIO
Mahindra & Mahindra — Hitesh Mulani, *Group Chief Information Security Officer & Vice President - IT Partner Collaboration & Process Excellence*

48 12. THE FORGOTTEN STORY OF "INSIDER THREAT"
Wipro — Sridhar Govardhan, *Chief Information Security Officer*

57 CONTRIBUTOR PROFILES

Securing Cyberspace is Key to Success in the Digital Age

Electronic version of this guide and additional content available at: SecurityRoundtable.org

1

How and What will they steal next?

Capgemini - Eric Anklesaria, Vice President & Global Leader Banking & Capital Markets Transformation

Security is an enabler in most scenarios unless one gets attacked and discovers newer vulnerabilities and threats. These are times when cybersecurity stops being an enabler that it ideally should be and becomes a disabler of sorts.

With everything, there is always a motivation. We need to ask the question of what exactly could be the motivations behind hackers attempting to steal confidential, priced information and what could be the greater societal and future impacts from such attacks. Is it merely monetary or are we looking at an attack that's personalized, sinister, and cynical all at once? Would our leaders across organizations react rationally or would that trigger emotional responses that could further exacerbate threats and vulnerabilities? What would be the far-reaching implications for executives, businesses, and eventually governments? I think before we dive into the what, let's look at the how part of future attacks

How?

There are different attacking modes and elements emerging from the growth spurt of several technologies. In fact, a lot of what could occur in future cannot be completely fathomed but can surely be estimated basis the trajectory of evolving technologies. Some of the technologies that we see evolving are (some illustrated in figure 1 below):

Figure 1: Possible Modes of Intervention

AI Algorithms: With the growth of cheap computing power and even cheaper storage availability, and our increasing use it will be a matter of time before a cyber adversary gets their our AI capability to launch autonomous cyber-attacks using AI based algorithms. Whilst the definition could be bantered around that we are there today, with exploit tool kits able to launch an attack after finding a vulnerability, this type of ability will increase over time. Training a machine and self-learn from their own attacks and improve themselves on the go. This will allow them to make decisions on their own without having to wait for orders and would be able to capture and destroy sensitive information without a trace. Time will tell how long this will become a reality.

Worms: The WannaCry attack of 2017 saw the first use of a worm in many years which allowed it to spread by exploiting vulnerabilities in the Windows operating system. Once installed, it encrypts files and demands a payment to decrypt them. It has two primary components: A worm module used for self-propagation and a ransom module used for handling the ransom extortion activities. This encouraged several cybercriminals to re-use worms for future attacks where automation and speed can be used to their own advantage. This would also substantially increase the probability of malware attacks in future.

Cloud Storage: The movement of data from on-premise models to off-premise cloud models will increase the chances for data exposure. 40% of data stored in the cloud is access secured which makes the entire data on the cloud vulnerable and prone to attacks. Cybercriminals have managed to compromise many cloud instances in part due to misconfigurations or lack of security controls. This has allowed cybercriminals to get access to privileged content and such breaches could involve people's data too.

What?

The future elements being stolen would also differ greatly from the current era as the importance of different parts of information could vary. In fact, our dependence on internet and connected devices continues to grow and this would increase the scope and severity of challenges and vulnerabilities. As attacks increase and get personal, users would perceive the internet as less safe to store information or even interact with.

Illegal Crypto Mining: The rise of cryptocurrencies in the market over the past year led to a new form of employment called Crypto Mining. Individuals and corporations are involved full-time in mining cryptocurrencies using compromised systems, even using servers and computing power available via servers at Amazon / Microsoft

/ Google. Whether they pay or compromise the virtual hosts, cybercriminals who understand this space turn unsuspecting users and their systems into the computing power for their covert individual mining activities.

What can we do: We can build awareness amongst users and admins, install software for detecting vulnerabilities in the cloud and for end points and updating monitoring tool regularly.

Enterprise Software Breaches: The increasing use of enterprise softwares (SAP, Oracle, Microsoft…etc.) across organizations that have overarching control over several functions of a firm are ripe for exploitation and manipulation. These attacks are far tougher to spot as it targets end users and does not usually depict a specific pattern or anomaly that's easily identifiable.

What can we do: We can build awareness amongst users and admins, conduct regular security audits and vulnerability assessments, install software for detecting vulnerabilities within the enterprise software and updating monitoring tools regularly.

Physical Infrastructure Paralysis: A critical attack pattern for the future would involve digital attacks by one country to disrupt the patterns of another also known as, Cyberwarfare. These attacks could be aimed at reputational damage, economic damage or even death in certain cases. Such attacks will run in parallel to traditional attacks that involve guns and missiles. The reason this is done is because no more than in the past computers control real-world infrastructure like airports, power grids, dams …etc. and hence, it is in theory more cynical to break the infrastructure – as simple as traffic signals and rail lines which could ultimately leave a country in chaos and render it paralyzed to attack or do anything in future.

What can we do: We need to take a strategic long-term approach, strengthen physical infrastructures through simple fixes in places (as simple as a pressure relief valve in a nuclear plant), and have a broader cybersecurity framework that makes the infrastructure not just secure but immune.

Implications

This is the most exhilarating part to unravel but also the most ambiguous. The implications of full-fledged attack sequences could hamper executives, businesses, governments and involve reputational, socio-economic, and financial damages many of which could be irreparable for a few years and could render nations useless leave alone organizations. Some of them are highlighted below:

Personal: A topic that gets least discussed on most future cyber threat planning seminars is the consequence of identity theft. Imagine your media accounts, bank accounts, employee access, personal achievements, academic credentials and everything related to you being stolen. This is damaging on several levels and could destroy one's life completely.

Economical: The losses related to finances could arise from the theft of bank details, disruption to trading, theft of money or corporate information. Such activities could destabilize the basis economic parameters by affecting liquidity, driving up/down interest rates, and ramping up inflation amongst currencies that are already weak at the global scale.

Reputational: Trust is the most important element that would be broken because of successful cyber-attacks. Erosion of trust amongst customers could potentially lead to: loss of customers, sales, impact suppliers, hamper partner relationships, and eventually diminish overall profits.

Banking Risks: If the victim is a financial services firm, economic consequences can be even more serious as was observed in the financial crisis debacle. The problems resulting from a central bank being hacked could

be far larger and could transcend to liquidity problems for other banks to eventual bankruptcy of borrowers from local banks and negative spillover effects on several entities that are part of the ecosystem.

What can we do: We can build awareness amongst users and admins, and build a robust cybersecurity framework, government policies that will help address all the implications above.

Conclusion

In summary, the future is packed with unknowns that can't yet be predicted or planned for completely but needs to be estimated via past patterns and analyzing motives behind attacks. We need to educate our users and our admins on the possible threats, perform regular cyber security assessments, and remain prepared for a quick response in the event of an attack.

The optimal strategy to a future cyber threat is hence, at minimum a trilogy of AI enabled technology, an evolving competent workforce, and an agile business model that could adapt quickly before or after an attack as required.

References:

1. Forbes Website; 2018
2. Capgemini Financial Services' Reports; 2018
3. Invest Northern Ireland Website; 2017, 2018
4. Global Risk Insights Website; 2017
5. IT Governance Website; 2018
6. Internet Society Global Internet Report; 2017
7. Tech Republic Website; 2018

2

Prioritising Cyber Risk for the Cyber Savvy CEO

Cognizant - Saritha Auti, CISO, AVP Cyber security

Cyber Security is a board room concern as emerging threats and exploitable vulnerabilities cast the shadow of risks on the business processes and surrounding ecosystem. Stringent controls emerging from need to protect the data (GDPR, CCCPA etc..) and geo political situations (such as Brexit) add to these concerns. There is always a dilemma on the cost of security versus cost of a breach which is extremely difficult to quantify to prioritize and justify the security initiatives. This is also something that each business needs to understand their cyber risk appetite. How much are we willing to lose/accept?

Information Security and Cyber Security

Information security is about securing the data residing in various systems, applications and database any organization will have. Historically, the context that drove information security were the boundaries and controlled access to the data. This meant having a robust firewall at the network boundary, IDS/IPS, identity management solution and probably database security did everything in the ecosystem what is required to secure the information. With fading boundaries and business making their data even more accessible, it drove a need to move beyond system or permiter based security to more of a data driven approach.

The construct of cyber security is around the data flows and business processes which have no boundary, which makes it very difficult to deploy on premise security solutions and control the security posture of a business process which extends outside an organization's network boundary. This includes all facets of security including physical and environmental security. Example of such an ecosystem is a combination of public cloud, private cloud and partner ecosystem where the data resides and consumed across multiple environments, protected with authorized physical and logical access, with staff skilled to secure the environment,

with right controls in place to protect the data across geo and business boundaries.

Key challenge the Organizations face are

1. How to get a unified view of security posture?
2. How to assure resilience of a business process?
3. How to be compliant across a business process?
4. What controls assure the security of data or a business process?
5. How to reduce the attack surface?

Unified view of security

Majority of Organizations have grown their security infrastructure organically and have many views of security posture – at network level, database level, application level, identity layer etc.. Most important aspect of security posture is to simplify the existing ecosystem and enable the seamless interactions of business processes with latest technologies and concepts.

Unified view of security depends on the maturity of security processes, technology, integration landscape and metrics in an organization. Creating a unified security view requires seamless integration between all teams: enterprise architects, application development, infrastructure , security and privacy team to lay the foundation of what needs to be reported as part of security posture and metrics. Example: integration of endpoint protection solution with enterprise authentication and authorization, network security components, Cloud access security brokers and security event monitoring and correlation engine, with Analytics and Intelligence solutions will provide a holistic view of security around data flows.

A good starting point is to understand if there is a handshake between the various teams driving technology in the CIO and CISO Organization to recognize and address technology risks and design decisions? Is QA Process include Non Functional testing? Have metrics been defined and being reported?

One approach the organizations can adopt is, to review the applications landscape to identify the data flows and business processes to secure in alignment to the organizations security policies and standards. Invariably the hosting environment also comes under the purview of these policies and standards.

Components of Unified security posture

Critical components of unified security posture are:

1. **Visibility & Intelligence** which the security technology brings onto the ecosystem to listen, qualify and correlate the network behavior as the data packets travers through the various infrastructure and application components.
2. **Contextualization** of network behavior to qualify the behavior as the deviation from the expected behavior at that instance (identification of anomalies)
3. Qualify security events as **Incidents** to trigger the security incident response process
4. **Risk qualification** of anomalies and trending of **Cyber Risks**
5. **Security incident trends**
6. **Threat patterns** based on external threats and internal security incidents correlated with organization's risk scoring mechanisms, resilience parameters and security awareness scores
7. **Persona based Risk views** for the executives to see and understand the posture

Compliance to standards

Compliance controls can be overwhelming if not handled well. Controls and standards need to be contextualized to address the business and geo boundaries, protect the data adeptly as required. Most of the organizations have multiple sets of controls and standards developed over a period of time. It is advised to review these sets annually to simply or consolidate, translate these controls into statement of applicability and implementation guidelines.

For example: Article 25 of GDPR requires data protection by design and default. This means, the data in any form (stationary or in transit) must be protected to ensure PII is securely stored. This may relate to other controls implementations from Sox, HIPAA or PCI such as Segregation of Duties, Infrastructure and Database design, security log collection and monitoring controls. It is always easier to map the controls across various regulatory requirements before deploying every control on the ground.

Assurance

Often CISOs get questioned by the Organization– how secure are we? This question has NO answer, even if the Organization has deployed all controls and have the best of technologies to protect.

Few examples which have direct impact on the level of Assurance which CISO can commit on security posture

1. Knowledge and awareness of the people on the ground which is delivering the applications and infrastructure in production
2. Exceptions which were approved and not tracked
3. Architecture and design errors – design decisions which were not justified by data points
4. Operational errors - Human errors, failure of automated process, failed upgrades/ patches/configurations which haven't been tracked or reported
5. Culture of the Organization

In the millions of transactions every organization will process, some of these are often ignored or missed which can bring down the business. Cyber security is the protection of information systems from damage or theft. In other words, cyber security is a subset of information assurance. Information assurance is an area that is formalized, and focuses on availability, authentication, confidentiality, and nonrepudiation.

Reducing the attack surface

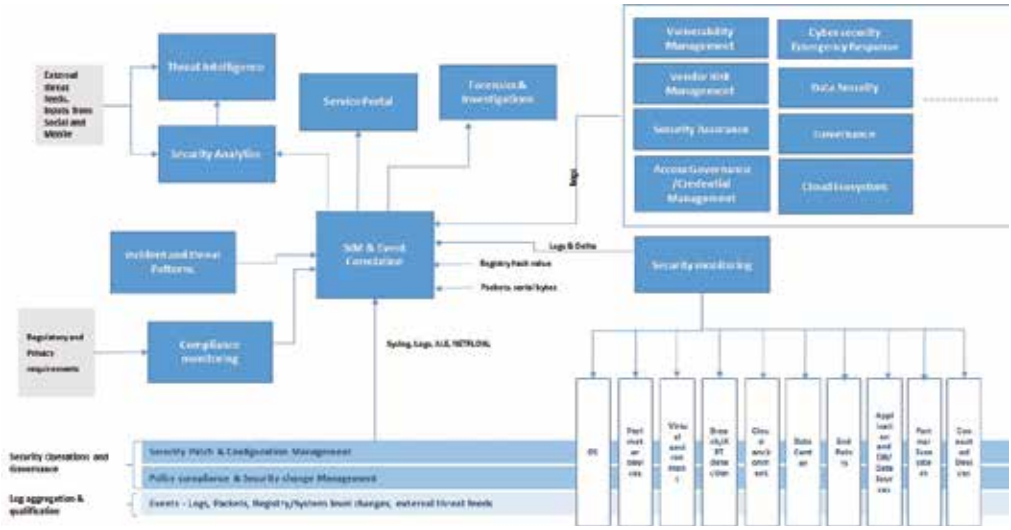
Attack surfaces increase with business expansions, mergers and acquisitions. To reduce the attack surface, key requirement is to know the ecosystem and understand the scope of reducing the attack surface. Simplifying Infrastructure is the crux of reducing the attack surface and helps simplify the security ecosystem as well. Feedback mechanism, error free operations help to reduce the attack surface.

Organizations should take 3 step approach to Cyber Security

1. Simplify security landscape – within the scope of Organizations
2. Secure using visibility, insights and intelligence – within the scope of business processes, including Partner and third party ecosystems
3. Sustain security using automation and operationalize using collaborative bots, analytics and threat patterns – within the scope of the business process

Operationalization of Cyber Security

Cyber security operationalization needs a holistic approach to integrate technologies, process and logs which matter in the cyber security landscape (as illustrated in the diagram here). Security operations is repetitive in nature and can be easily automated. Every process with a fixed input and a predictable output should be considered for automation.



Shifting the paradigm CIOs

CIOs should be included in security strategy discussions, privy of the fact that he/she needs to invest time in reviewing security programs as they sign the Enterprise Risks.

CIOs need to think security by design, as they run their Information Organization. This means every program they initiate should have all components of Cyber Security including Secure SDLC. CIO's also need to look at reducing the cost of operations by simplifying the environment, use "Security as a service" offerings as applicable, use bots for handle repetitive processes on security operations, parse through tons of alerts and false positives to determine sanctity of an alert.

3

How Data Grids Will Power the Economy and Influence Our Future

Data Security Council of India - Rama Vedashree, Chief Executive Officer

In less than two decades, since the beginning of the third millennium, digital data has transformed everything.

It started with the sheer volume of data, which became multiplied by the many digital formats and media forms. The internet and cloud have enabled digital data to become connected into a global data grid, which has enabled us to gain intricate insights into one another, as well as how our world works, plays, interacts, and governs. It has reshaped the very nature of our communities at the local, regional, and global levels—enriching our economies, enabling collaboration across the world, and allowing us to enjoy more productive lives at work and at home.

In turn, accessibility to this cyber mesh of connected and connectable data has elevated the potential for cyber risk and "digital deluge." It has created an important sense of urgency for an ecosystem of enablers—governments, enterprises, educational institutions, and advocacy groups—to work together toward the common goal of making our digital universe safer.

When I took on the role of CEO of the Data Security Council of India two years ago, I was optimistic about the commitment of interested stakeholders in ensuring that the digital economy and, in fact, our digital lives, would be safe and secure. However, a number of factors are coalescing to give us concern. The fast-paced digitization momentum across the world, rapidly growing economies like India's and China's, and the recent World Economic Forum's "Global Risks Report 2018," which cites cyber risks and data theft/fraud as global risks, are together a wake-up call for action at the global, regional, and national levels.

Still, two years later, I am even more optimistic about our ability to harness this massive wave of data, in all its many forms and connections, for the good of our global societies. Of course, I am also realistic about the need for

intelligent cyber risk identification and mitigation practices in order for us to build and prosper from the "digitization of everything."

At the core of this ability to build and benefit from a cyber mesh of data are five key concepts:

1. Developing a global data grid to shape and fuel the global economy.
2. Using data as the new currency for today and, especially, the future.
3. Weighing the ramifications of Big Data in shaping the enterprise and consumer of the future.
4. Balancing our innovation ecosystem with the reality of data monopolies.
5. Enabling cybersecurity and privacy imperatives to co-exist in a data-driven world.

Where we go from here is dependent on a whole host of factors, many of which have yet to emerge and are difficult to predict with certainty. But we know this for sure: Digital data is going to change the world in even more dramatic ways than it has done since the invention of first-generation computing.

Data Grids: Powering the Global Economy

The concept of grids—interwoven, mesh-like systems and processes for a wide range of industries and applications—is well known and widely understood in our societies. Grids exist and function smoothly for such applications and sectors as power and electric, financial systems, aviation, and many others.

Now, a new type of grid has emerged—a global data grid—which merges the tremendous surge of information with all the connected points in other grids. This cre-ates exciting, powerful business models that weren't available just a few years ago. For instance, think of how the free flow of data across physical and digital storefronts has spawned the age of multi-channel retailing that knows no geographic boundaries.

Global data grids also exist for the amazing growth in user-generated content—everything from social media platforms, wikis, blog sites, and personal e-diaries—that encompasses everything from family genealogy and hobbies to open source software communities.

In global data grids, information will increasingly be shared from sector grid to sector grid, promoting increased collaboration that utilizes common information or generates new insights from previously unseen data. This will rapidly evolve into a global, real-time data grid, with companies, government agencies, and consumers collaborating on data creation and access.

Think about the promise offered by data-centric compliance mandates, such as the U.S. Health Insurance Portability and Accountability Act (HIPAA), which allows patients to take their personal health information with them, regardless of which doctor, medical facility, insurance company, or healthcare service they use. Now, multiply that potential exponentially across industries and around the world. We see similar global data grids being formed in areas such as higher education, tying together both physical and virtual learning centers, as well as university-sponsored research laboratories, public policy think tanks, and community development programs. Consider, for instance, the increasingly global footprint of major universities, such as Harvard, Stanford, Oxford, and Le Sorbonne—all of which have built and are leveraging their own global data grids.

That is where we are going.

Data As the Currency of the Future

A generation ago, there was a lot of talk about, "Oil as the new currency." Today, however, there is increasing evidence that data is, in fact, becoming our new currency; and that trend is likely to accelerate. Consider these data points from industry research:

- By 2020, the value of the European Union data economy is projected to hit 739 billion Euros, representing 4% of European Union gross domestic product (GDP)—more than double its portion of GDP just five years earlier.[1]

- "Digital industry"—global data-centric market segments—will increase its annual profit margin potential by more than $1.4 trillion annually by 2030.[2]
- Digital transformation will contribute more than $1 trillion to the Asia Pacific GDP by 2021, driven heavily by artificial intelligence, the Internet of Things, Big Data, and other data-driven initiatives.[3]

Of course, trying to get a handle on the financial contribution of digital data isn't new. In fact, global consulting giant McKinsey wrote about this issue as far back as 2013, when it raised the notion of separating the economic impact of digital capital from that of tangible technology assets, such as hardware, software, and IT-enabled services.

It is clear, however, that it will not be long before we no longer are writing articles or papers with the headline, "Data is the New Currency" for a very pragmatic reason: Data is rapidly establishing itself as the currency of record for all global industries. It is, in fact, becoming the "new oil." In healthcare, financial services, manufacturing supply chains, retail, utilities, government services, and in all other market sectors, data is being monetized in a wide range of applications. And we have only tapped the surface.

Perhaps typical of the impact of data on markets, industries, and economies is a recent blog post by banking industry consultant Chris Skinner, who wrote:

"If all the things we used to do (in banking) make no profit anymore, where is the money to be made in the future? And the answer is: data."

The Big Impact of Big Data Will Get Even Bigger

It is easy to be amazed at the massive growth of digital information. The much-discussed Big Data movement is now mainstream, and it has enjoyed enormous popularity as organizations learn how to harness this growing amount of data for a wide range of use cases.

But the sheer volume of data growth is not the issue. Organizations need to find new ways to efficiently access the right data from the right point in the global data grids in order to make a real difference in how we work, play, and interact. Without a strategic plan—and the right tools—for harnessing all that data, organizations will drown trying to "drink from the fire hose."

Big Data—augmented by related data-generation trends, such as mobility, wearables, virtualized infrastructure, e-commerce, IoT, distributed workforces, collaboration platforms, enterprise content management, and others—has only begun to scratch the surface of what it can do. That's due to a number of factors, such as the formative stages of data-mining tools and the early development of powerful, secure algorithms that turn raw data into actionable insights. Big data's growth, as impressive as it is, also has been limited by enterprises' desire to keep capital expenses as low as possible, which is problematic for Big Data use cases that require more compute power, more storage capacity, more net-work bandwidth, and more data centers.

But as prices on IT infrastructure continue to fall, and as cloud service providers become the new data centers for large and small enterprises alike, Big Data will accelerate its ability to capture, store, manage, analyze, and share data from a wider and more diverse set of inputs.

Take healthcare as an example. To say that data is exploding in the healthcare space is stating the obvious. One recent study said healthcare data is growing faster than ever—nearly 50% annually.4 That is due to a variety of factors, including regulatory mandates, digitization of healthcare business processes and workflows, the rise of applications such as telemedicine, and the insistence of healthcare practitioners on using their own personal devices to create and share information about their patients and their practices.

Healthcare is just one prime example of an enormous opportunity for improvements, touching on both patient benefits (in the form of improved medical outcomes and better long-term health) and commercial success for

hospitals, practitioners, and insurers. Public health, for instance, is a fast-growing specialty that relies heavily on data from across the healthcare data grid, as are other exciting use cases, such as global telehealth practices and infectious disease control. And applications around medical imaging, such as PACS and DICOM, are in the early stages of both commercial opportunity and dramatic improvements in patient care. Managing radiology images and other unstructured data in a global healthcare grid is literally a life-saving development and helps realize the vision of universal healthcare.

Whether it's healthcare data, information about banking transactions, up-to-the-minute feeds on traffic congestion, or real-time insights into the health of common household appliances, Big Data is going to reshape the very nature of how organizations in all industries do business and serve their commercial and consumer customers. For example:

- Analytics engines are going to become considerably more powerful, more affordable, and easier to use, often integrating with analytics engines of social media feeds and other consumer platforms.
- Consumers will make real-time decisions based on multiple data feeds shaped by independent—yet connected—analytics engines. This will expose them to more new products, services, suppliers, and relationships than ever—and they will not have to invest a dime of their own money to take advantage of those analytics engines.
- Delivering services to commercial and consumer clients will become faster and more personalized than ever, improving the user experience and driving enhanced customer satisfaction— leading to even more consumption.

As that happens, the Big Data trend we're currently experiencing will not seem so big after all, compared to what we will experience in just 5 to 10 years from now.

How big could it be? Consider the fact that the worldwide population stands at about 7.5 billion people in 2018. Now, how many "things" do each of us use every day that could have important information that we access or share? 10? 50? More?

Are Data Monopolies and Innovation Mutually Exclusive?

With so much attention and energy stemming from important developments, such as the internet, social media, and cloud computing, it should come as no surprise that "data monopolies" have emerged— disproportionately large collections of data held and managed by a handful of innovative, ambitious, and powerful enterprises.

The commercial success of companies like Facebook, Google, Twitter, Amazon Web Services, Alibaba, Tencent, and other industry titans are remarkable examples of the combination of smart business decisions, commitment to innovation and research, bold bets on new technologies, and a little bit of good luck. The fact that these and a relatively small number of other organizations collect, hold, and leverage massive amounts of data is not, by definition, something to fear. It is, of course, something to acknowledge; we must understand its implications.

After all, the broad collection of personal data undoubtedly sparks concern over privacy rights and confidentiality. That was a big driver behind the European Union's landmark General Data Protection Regulation (GDPR), which may influence and shape data privacy regulations in other regions of the world.

And, if data is the new global currency, it's not surprising that some people are raising concerns about "whoever controls the data has the power." But there is an important balance that needs to be struck between preserving the privacy of individual data and allowing businesses and governments to use data in a responsible, innovative way to better serve their constituents.

This is not a black-or-white issue. It's highly nuanced, with the need for a delicate balance to ensure that protecting data doesn't lock out innovation, or that harvesting data to create new goods and services

doesn't imperil our individual identities and rights.

The tension among companies, governments, regulators, and consumers is inevitable, with each group trying to promote its own interests. But we need to keep in mind that this doesn't need to be an "I-win-you-lose" scenario.

We also need to understand the appropriate role of government in protecting individual rights and avoiding the deleterious effect of data monopolies. Our governmental agencies and regulators should avoid going down the path of heavy penalties and overly regulated data access and usage, opting instead for collaboration among all stakeholders to strike that delicate balance between commercial innovation and individual privacy of personal data.

In fact, I believe industry players will increasingly band together to collaborate on smarter, more efficient compliance protocols, and will team with government agencies, regulators, privacy advocates, and standards bodies to do so. While this may seem like an unusual alliance, I believe it is a more efficient and effective way to ensure responsible compliance measures without stifling innovation.

Protecting Our World and Our Data Against Digital Threats

As excited as I am about the possibilities of using all this data for the common good of our societies, I am also realistic about the growing footprint of cyber threats. Every year, the incidence, impact, and innovation of cyberattacks increase, and there's no reason to think they will abate in the coming years.

Again, data—and proper access to it—is key to ensuring that applications, services, and entire economies are safe and secure. If that sounds like "data that protects data," you are right. In order to protect our most important data—personally identifiable information, financial records, medical records, intellectual property, and more—we will need to develop new tools and services to discover and remediate data vulnerabilities.

Yes, threat intelligence and other subscription-based services help to identify threats and promote joint problem solving. But we need to do more. Too often, we have incident feeds that are limited in their impact or ability to promote remediation because they lack access to critical data about threat sources, points of attack, weak points at the network's edge, indicators of compromise, and more.

Again, the notion of balancing security needs with privacy expectations is relevant here. But it goes even farther. After all, there's nothing preventing us from locking down everything tighter and tighter— servers, mobile devices, applications, cloud services, and more. Doing so, however, seriously degrades the user experience and stifles innovation in data-driven goods and services.

Data must continue to flow, reliably and securely, through networks that are increasingly global and susceptible to the efforts of bad actors. Restricting data traffic to the point of choking it impacts our data economy locally, regionally, and globally. That's why the European Union is working on regulations to unlock the data held by European institutions, and the U.S. federal government has an open data initiative.

This concept is evident in the rise of data marketplaces, or data supermarkets, which enable new companies to build markets where public data is available. In these scenarios, specific users can easily combine that data with other, free data sets for improved insights and unearthing new business opportunities and societal value.

Ensuring this cross-border data flow is going to require a more collaborative effort among commercial, governmental, regulatory, and consumer bodies. In fact, to promote best practices in cybersecurity and to protect individuals, businesses, and governments, we must find ways to promote more data sharing and greater collaboration. Take terrorism, for example. Fighting both physical and digital terrorism requires cooperation among a vast network of agencies, organizations, and data sources, all around the world. We must continue to push for

ways in which governments, particularly in areas of law enforcement and national defense, work together.

We should also strive to step up deliberations and consensus building around the application of international law and governing states in cyberspace, at both the UNGGE (UN Group of Governmental Experts) and bilateral levels. The recently mooted "Digital Geneva Convention" and other proposals need attention to ensure that states do not violate established norms in cyberspace. This is necessary, not only to identify and weed out cyber criminals, but also to protect and preserve individual liberties, particularly as many governments have built offensive cyber capabilities.

In an era of digital economies and digital lifestyles, we need to treat security as a core feature and requirement in all products and services, from the onset of the design phase. Our communities, economies, and constituents demand it, and it will be on our hands if we don't deliver it.

Conclusion

Our societies and our lives have been dramatically impacted by developments as basic as the discovery of fire, as well as simple and complex inventions such as the wheel and hydroelectric power. But I believe there is no development with greater long-term implications for our world as new applications for digital data.

Data is more than seemingly random collections of ones and zeros. It is information, currency, social fabric, safety, knowledge, confidence, and innovation. When created, shared, and managed for the good of our communities, our families, and our industries, it acts as an exhilarating source of hope for a better world. And when combined with smart, collaboratively developed security safeguards, it gives our best and our brightest the opportunity to continue to use data in heretofore unimaginable ways for the common good.

Technological advancements may allow us to connect more things to each other, but the real power and beauty of a connected society is its ability to use grids of data to bring us closer together as people, as communities, and as nations.

References:

1 "Building a European Data Economy," Digital Single Market, 2017

2 "Digital Industry: The True Value of Industry 4.0," Oliver Wyman and Marsh & McLennan, 2016

3 "Digital Transformation to Contribute More Than US$1 Trillion to Asia Pacific GDP By 2021," Microsoft and IDC, 2018

4 "Report: Healthcare Data is Growing Exponentially, Needs Protection," Healthcare Informatics, 2014

4

Winning the Cyber-Security War Requires a Truly Collaborative Effort

Deloitte India - Shree Parthasarathy, Chief Innovation Officer, National Leader - Cyber Risk Services

The Digital Era is firmly upon us and as we hurtle down the digital highway, not at a pace of 5G but more at warp speed, organizations are embracing digital technologies to advance their businesses or just even to stay relevant.

In this era technology has emerged as a common denominator, a key enabler, a disruptor and as well as a growth driver. According to Gartner, worldwide information technology spending is expected to touch $3.8 trillion in 2019. More than ever, people, organizations and Governments don't seem to have much choice, but to adopt digital technology and transformation exercises to empower them to survive, changes and morph into models that will make them resilient for the road ahead. Further in the new era, with the data explosion they are finding ways to put this data to better use and mining it to derive useful actionable insights and enhance experience.

The confluence and ubiquity of these technologies has had a profound impact on our experience as a person (customer, employee, supplier, stakeholder etc.) organization, government etc. the way we live, work, and play. It has opened up a plethora of opportunities for businesses, however it has opened up a whole new world of digital risk and also thrown up some complex security challenges.

As we embrace the onslaught of acronyms and exponential technologies i.e. the world of AI, IOT, Mobile, RPA, Cognitive, Big Data etc., and adopt them within our environments we're increasing the threat surface by exposing more areas of our infrastructure and business environment to cyber risks.

We have now entered a very different and complex realm as far as security is concerned. There has been a paradigm shift given the unprecedented number of connected devices, infinite exposed threat surface and enormous volumes of sensitive data that need to be protected. This number is set to explode over the next few years. IDC has estimated that there will be 80 billion connected devices

in 2025, generating 180 trillion gigabytes of new data in that year.

For an organisation this means that there are so many more vulnerable end points that are available to attackers who wish to disrupt the organisation and these threat vectors are much more complex. It's no longer a single hacker sitting in his basement and trying to create trouble. Instead, we are seeing far more sophisticated attacks that leverage the growing importance of data. The motivation for hacking could range from corporate espionage, government-driven cyber wars, terrorism, or criminal intent. In such a scenario, our traditional cybersecurity measures prove to be woefully inadequate. For example creating of smart cities may provide lot of convenience to our citizens, however the same smart city now has exposed it's underbelly (offline resilient infrastructure) to cyberattacks, if security factored in. Similarly a manufacturing organization automating its production environment using Industrial Internet of things ('IIoT') has exposed itself to a new type of risk, which has the threat of disrupting its entire manufacturing and production.

Security companies that provide tools and technologies and security professionals now need to embrace this new reality rapidly broaden their tools and skills beyond IT security, and extend it to cyber security and protect any device or equipment that generates a 0 or a 1 (i.e. cloud, IoT, mobile, physical security devices, PLC's, drones, operational technologies etc.). Further for these new infrastructure they need to identify the exposures or cyber risks and test/devise well-crafted strategies to address both known and unknown threats. Gartner predicts that by 2020, 60 percent of digital businesses will suffer major service failures. In large part, this will be due to the inability of their security teams to mitigate digital risk. Any security breakdown is likely to have far reaching consequences on both productivity as well as reputation.

While companies are struggling to cement their security infrastructure and they deal with breaches on their own, and given the stigma and reputational damage that comes with any reported breach, organizations seldom report the same. This attitude is understandable considering the negative sentiment, however it is extremely detrimental to the future of security. Since sharing of such information generates early warning signals for other organizations and collectively the Government and organizations can thwart a much larger breach by hackers. However regulators and governments need to make the environment conducive and supportive to encourage organizations to share such information. Organizations need to realise that collectively we are much stronger and have a chance to fight hackers who have abundance of resources.

As threats spiral and there are more global incidents across sectors, regulators across industries are getting jittery and are scrambling to protect shareholder value. This is resulting in not well thought out counter measures , which is resulting in imposition of highly impractical and draconian regulations that severely limit the value of the IT & Digital infrastructure. It is akin to throwing the baby out along with the bath water. This has a severe impact on Digital transformation and the outcomes it can deliver in the areas of experience, productivity, efficiency, and competitiveness etc.

What is needed is a well thought out multi-pronged strategy and approach that takes into consideration risk and rewards and encompasses people, process, technology and facility. More importantly, for any solution to be effective, it needs to encompass the entire value chain and all entities in the ecosystem including enterprises, vendors, partners, government, consultants etc.

So the question one needs to ask is, what can the industry do to ensure that cyber security moves at a much faster pace?

The Good Guys Need to Band Together

This reminds of an old story of bundle of sticks, where when you take a stick by stick, it is easy to break them, however when you tie them into a bundle they are very difficult to break. Similarly incident or breach information is not shared and hence across sec-

tors, organisations or countries and this aspect of not operating in the collective is making organizations easier targets for hackers, who most often go after the weakest link and in some cases there are bounty hunters who go after the strongest link and where they believe there will be the most reputational damage

There needs to be a sense of urgency to find common ground across various stakeholders (The good guys) of the ecosystem - government, private enterprise, academia, consultants and regulators. There is a need for a common global security and risk framework that is developed in a collaborative and inclusive manner. The world today cannot afford to make the same mistakes that we made while setting specifications for electricity. Each country / regions now have different electrical specifications, sockets and compatibility issues, all of this is helps no one.

A common standard for security is key to fighting global scourge of data theft and breaches. The security industry could take a leaf out of technologies such as cloud, block chain or IoT that have managed to set fairly consistent global standards. On Blockchain, for instance, in India a consortium of banks have come together and are working towards create a common security standard. So shouldn't we do something similar on cyber security?

At the same time, we need to encourage a culture where organisations proactively share details of breaches, so that the rest of the industry can take note and act. Hackers often use some standard techniques to launch their attacks across different organisations. Threat intel from one breach operates as an early warning signal and this can help organizations develop counter measures and be invaluable to the industry as a whole. Setting up a viable mechanism for organisations to report breaches without fear of retribution will be extremely crucial. Unless information is shared freely, tackling data breaches will be near impossible.

The question of who should own this collaborative initiative is up for debate. While the Government may be a natural choice, past experiences have indicated that it might be ill-equipped. For example, cyber laws in India are archaic and don't cover the latest technologies. Further the police departments are not trained to deal with complex cyber-crimes. Therefore, the best approach will be for regulators, private enterprises and academia to come together in a PPP model and conceptualise a viable, robust system that works.

Security vendors too need to play a role in facilitating common standards. While each vendor certainly needs to build its own differentiators to maintain a competitive edge, there needs to be a commitment to common protocols and alignment at the network, communication, data and sensor layer. A combination of Open Standards, Open Source technologies and a Public Private Partnership (PPP) model is the way to go.

In the US, the NIST Cybersecurity Framework provides guidance on how private sector organizations in the country can assess and improve their ability to prevent, detect, and respond to cyber-attacks. A similar initiative in India as well as at the global level is much needed. Given the magnitude of this problem, trying to solve it at an individual organisation level is setting yourself up for failure. More organizations and cybersecurity experts need to join forces and develop a common language, so that our collective defences grow that much stronger.

Establish a Large Pool of Skilled Security Ninjas

The fight against data breaches requires a new breed of security professionals who not only understand the technology, but also have adequate insights into how businesses run. They also need to understand and appreciate the urgency when it comes to securing an organisation. Unfortunately, the dire shortage of trained information security professionals is a reality today. While the industry needs about five lakh professionals to be trained in security each year, the actual number on the ground is less than a lakh.

This skills shortage needs to be tackled on a war footing by the industry as well as the government. Organisations need to put

together comprehensive training programmes to develop in-house security talent. There need to be targeted training programs for professionals at a large scale.

While this approach is important in the short term, we also need to think long-term. Information security training can start right at the school level. Teaching kids the importance of information security and training them to write code is important.

The industry also needs to tie-up with educational institutes and universities to ensure that the academic curriculum is up-to-date and reflects on-ground realities. Centres of excellence within universities can help drive innovation too.

Prioritise Security is Key

As discussed before, the number of connected devices and the quantum of data generated have gone through the roof. For instance, statistics show that the demand for smart speakers grew 43 percent just in the second quarter of last year. The number of wearables shipments in India hit the one million mark in August last year, as per IDC.

In this situation, it is humanly impossible to find the looming threats through traditional methods. One classic example that I like to use is that of someone attacking you with tennis balls. If there is one ball, you can catch it. Same with two or maybe three balls. But what do you do when someone attacks you with a 100 tennis balls? Or a thousand? This is the kind of data explosion facing the security industry today. To counter the security threat at this level, what we need is a well-crafted combination of big data, predictive analytics, automation, and anomaly detection AI.

Unfortunately, most organisations simply choose to ignore the threat and hope that it will go away. Burying your head in the sand like an ostrich, hoping that the sandstorm will goa ways is not a solution. This will only make the problem much worse and will cause exponential damage. Trying to use old solutions to a new problem is a perfect recipe for disaster.

The other approach of delaying digital adoption to limit exposure is also a short-sighted approach because it will significantly hamper growth and cause a slowdown.

The problem we are dealing with is very complex. Ensuring watertight data security, while also respecting individual privacy is a very tough task. Only a collaborative approach and secure, vigilant, and resilient solution is the key to solving this.

And we need to do this because it threatens our very survival!

Sources:

https://www.gartner.com/en/newsroom/press-releases/2018-10-17-gartner-says-global-it-spending-to-grow-3-2-percent-in-2019
http://www.vebuso.com/2018/02/idc-80-billion-connected-devices-2025-generating-180-trillion-gb-data-iot-opportunities/
https://www.hindustantimes.com/tech/alexa-turns-1-in-india-amazon-bets-on-voice-third-party-devices-for-growth/story-0llSzX1VDxyBPypjb3Uf6H.html

5

Weaving Security Into The Fabric of Global Digital Buisnesses

GENPACT - Ramachandra Hedge, Vice President, Chief Information Security Officer

Cybersecurity as a Business Risk

Cybersecurity is a business risk that can impact an organizations profitability, operations, reputation – just like any other business risk that needs to be managed. There are some specific characteristics of cyber risk that are unique i.e. relative immaturity given information security risk management is a young discipline and global standards are still evolving. Also unlike say physical theft where an intrusion and theft of an asset is easily evident, copying and exfiltration of digital data is inherently less easily detectable. Further, with the global nature and inherently insecure design of the Internet, attacks can be carried out from across the world, and the difficulty of attribution (i.e. figuring out with a high level of confidence exactly who is responsible for a cyber attack, and what their motivations are) compounds the problem. Finally, a lack of consistent basic understanding and education of cyber risks, hype and misconceptions add to making this area appear extremely difficult to make sense of and navigate. Organizations that operate globally, in addition, have a maze of security and privacy related regulations to interpret and comply with.

Several of the solutions to the underlying issues of the current global cyber risk landscape i.e. policy aspects, structural issues with the Internet, standards and regulations, product liability enforcement, cooperation between countries, are beyond the scope of most organizations, yet enterprises are caught in the cross-hairs of these risks and have to manage them, and the ones who do it well will not only have a higher likelihood of not being impacted, but might as well end up enhancing their reputations and business success.

So how does an organization go about managing cyber risk?

Firstly, by recognizing that the risks are real, and this is a critical business risk issue, not a technical IT problem.

There are a variety of threat actors who have different motives, ranging from stealing sensitive information or conducting fraudulent transactions for monetary gain, to other objectives for stealing intellectual property or causing disruption. While the type of business(es) the organization operates in can make it more susceptible to specific risks e.g. credit card theft in retail, IP theft in high tech manufacturing, organizations can be attacked as a "target of opportunity" if they are sloppy in their cyber hygiene and have left their systems vulnerable and exposed. Additionally, they can be collateral damage in broader attacks, or be attacked if they are a conduit to other organizations the attackers are interested in.

While most of the risk implications and resulting business impacts are fairly intuitive, this article will hone in on

- Some key foundational elements for a successful program, namely building the security structure and capabilities, fostering a business focused and risk based security approach and security culture, and focusing on hygiene and crisis management.
- Specific areas where cybersecurity considerations are increasingly important – mergers and acquisitions, digitalization, and supply chain.
- Risk Transfer i.e. Cyber Insurance, and finally a note on the interplay of Security and Privacy.

Starting with structure and capabilities

Having appropriate information security capabilities is a prerequisite for an organization to address this risk. This would mean having the right security leadership that is supported by senior management, and capabilities in terms of resources , budget and decision rights. While the specifics of the structure and responsibilities will vary by organization, generally the CISO and his/her team is charged with working with business and functional leaders to develop the security charter and strategy, provide updates and as needed educate and advise the Board and senior management, govern security processes, directly run critical processes, and more broadly orchestrate all the different aspects of security through the organization. While the CISO and the security team have to do their bit to establish credibility and demonstrate leadership, it is equally important that they are provided adequate support and backing by senior management, and the tone at the top is clearly set that security is everyone's responsibility.

For almost all organizations, the nature and sophistication of some of the threat actors mean that having strong partnerships with specialized firms and security partners, so they can be leveraged as needed for niche expertise, scale and intelligence, is essential, as is being plugged into the larger ecosystem i.e. industry and information sharing associations, government agencies etc.

Adopting a business focused and risk based security approach

While it is imperative for the organization to figure out specific cyber risks relevant to its business and have appropriate controls, it is equally important to ensure there is a focus on risk and business enablement. This means that the security teams need to have a good understanding of the business, are aware of what the organization's key priorities are, and are proactively engaged in key business initiatives and help securely enable them.

It is also important to draw the distinction between being "secure" in absolute terms, and having a risk based approach. And this ties in with the broader maturity level of the organization on risk management, where risk assessment, mitigation and most importantly risk acceptance processes and responsibilities are clearly defined. Beyond a point, investments in security controls can have diminishing returns in terms of reducing the risk, hence it is important for the organization to figure out where to draw the line.

Absent a business focus and a risk based approach, there is a danger that security professionals will implicitly assume their role is to accept and own the risk, and this could drive them to skew on the side of being overly conservative, or not distinguish

appropriately between differing aspects of business criticality, or not be proactively engaged in critical initiatives- all of which can have negative consequences – of security requirements and processes being set overly conservatively and frustrating users, causing delays or otherwise hampering business projects (vs proactively securely enabling them) , or worse of users and leaders of business initiatives perceiving the requirements as unrealistic and the security teams as "blockers" and bypassing controls or the security assessment processes.

Focus on doing security right, and compliance will largely be a byproduct.

An important aspect here is to not equate security and compliance. This is not to downplay the importance of complying with laws and regulations. Compliance regulations, particularly when coupled with effective enforcement have a critical role to play in helping drive baselines and practices in the right direction. However, no compliance regulation can be written to effectively deal with the specific security requirements of each organization and its risk appetite, and regulations often focus on enforcing specific practices and controls that might become less effective over time.

Organizations thus need to recognize that the right approach is to develop a security program that's appropriate for the business and managing the risks it faces, and if does that well, it will most likely discover that most of the compliance requirements are being met anyway, and while it would still need to take efforts to meet specific requirements of any particular laws, the process becomes easier and sustainable.

Weaving Security in - why culture is paramount

Users are a critical line of defense. Most attacks rely upon phishing as the first point of entry into an organization. While many phishing attacks look to exploit vulnerabilities and implant malware, several others rely on just tricking users – often by sending emails that purport to come from senior executives , and relying on human tendencies to respond to urgency, fear, intimidation or being kind and helpful – to trick employees into divulging sensitive information, initiating transactions to make payments etc.

Getting employees to understand that security is a business issue, and that risks are real for the organization, is critical. With the daily drip of news on cyber incidents, there is a risk of employees tuning out and experiencing what is called as "breach fatigue" , which can lead to an attitude that nothing can be done about the problem. At the other end, others can become overly paranoid and worry about the wrong risks. Finally, It is still not uncommon to think of information security as largely an IT issue, one for the information security and IT teams to deal with, as well as to have the perception that their particular organization will not be attacked or targeted.

Not having the organization educated, and employees attuned to the risks and their roles, can have significant consequences- from users being more vulnerable and succumbing to attacks, to not reporting incidents, to not engaging proactively with the information security teams on business initiatives.

Additionally, while actions of employees or the "insider threat" get a lot of attention, the reality is that a lot of these incidents are not necessarily malicious, but are just made by employees who are not thinking through the risks, or have not internalized the business implications of not applying security controls and are thus choosing to take shortcuts.

Some of the solutions to these challenges are – ensuring that there is a process to educate all users on security and in having a balanced perspective on cyber risks, sharing data which is specific and relevant to the organization to drive home the point that risks are real, and helping users to make the right choices. Providing guidance that is useful to them in their personal lives also is likely to be well received by employees and helps drive the overall baseline higher. For global organizations, it also is important to consider cultural nuances and tune its educational program accordingly.

Getting the Basics Right

Having the right security hygiene can go a long way in fending off common and opportunistic attacks. Even if the organization is targeted by sophisticated adversaries, having the basics right raises the bar and changes the equation in an its ability to detect intrusions sooner, respond faster and minimize the impact.

What are these basics? These are common practices- promptly applying patches to systems, ensuring anti-malware technology is deployed on infrastructure, backups are taken and tested, user accounts are promptly revoked when employees or contractor leave the corporation, a basic level of logging and monitoring is in place, and that there are strong controls on privileged access. These sound like obvious measures, but breach after breach has reminded us that organizations are found lacking in implementing these basics.

What can sometimes be worse is having a false sense of security i.e. an organization thinks it is secure because it has deployed the latest technologies but they has not been correctly configured, key functionality is not enabled, or no one is monitoring the logs or reports. Making sure the security technologies that are deployed are optimally utilized and that all aspects – related processes, capabilities in terms of qualified and trained personnel are all considered and integrated into these projects is key. Technologies without the right processes and people will not deliver results.

Passwords have been demonstrated to be of decreasing utility, and particular, with users choosing to use the same passwords across services- which in itself is a poor practice, and with millions of user passwords already compromised in various breaches, the risks of "credential stuffing" attacks make reliance on just passwords even riskier. Using Multi-Factor Authentication (MFA) should now be considered as a baseline hygiene practice.

Incident Response , Cyber Resilience and Crisis Management

One of the biggest misperceptions is that a cyber incident is something that is to be handled by the information security or technology teams. While these teams undeniably have an extremely critical role to play in triaging the incident, investigating and driving mitigating actions etc., once an incident has reached the level of a crisis – it has to be treated just like any other crisis . Business leaders have to be deeply engaged and drive decisions, and other functions, e.g. legal, corporate communications also have integral roles to play.

How an organization responds to such crises is often more important than the actual incident itself, and unless the organization has crisis management procedures documented , including with specific aspects related to cyber incidents, which are periodically tested, this becomes difficult to execute during an actual crisis. While it is true that every crisis has different nuances, there are several common foundational elements that come into play e.g. forming the right crisis team and structure for decision making, having clear communication protocols, process for out of band communications, etc.

Conducting simulations and table top exercises goes a long way in strengthening the organizations muscle memory on these foundational elements, and during an actual crisis, frees up precious time and energy to focus on the specific matters as these foundational elements are executed seamlessly. Organizations that view cyber incidents as inevitable and plan for it will be the ones who will have greater success in managing them.

Mergers and Acquisitions

Post acquisition disclosure of cyber breaches in the recent past (e.g. Yahoo's acquisition by Verizon, Starwood's acquisition by Marriott) , have put a focus on the importance of including cybersecurity aspects into the due diligence process. The risks of uncovered cyber risks are not limited to just post acquisition discovery, disclosure and financial and reputational impact, but also as systems get integrated and networks get bridged, of threat actors getting access to the acquiring

organization and resultant exposure. Thus organizations need to ensure that cyber aspects are appropriately covered during due diligence, as well as before integration of systems.

Digitalization Efforts

As businesses embrace digitalization, the trend is inexorably for increased connectivity, sensors and computers embedded into everything – automobiles, factories, pacemakers, thermostats- termed the Internet of Things (IOT) as well as increased automation and connectivity in industrial and manufacturing systems (IIOT). A steady series of media reports on cybersecurity incidents - whether it is hacking into connected cars, denial of service attacks from compromised cctv systems, have served as a reminder that while organizations pursue and realize the undeniable benefits of digitalization, the risks, if not managed can have significant consequences. Fixing some of these issues e.g. having patients to visit a clinic to update implanted medical devices, physically changing settings on thousands of hotel room doors- can have significant costs or be downright impractical.

Organizations have to ensure that security is conceived at the design stages itself, and operational security is also equally important for IIOT systems. While the underlying principles of security will remain broadly the same, the approaches and methodologies that are applied to IT systems cannot just be forklifted and applied to IOT and IIOT systems. Doing this well will require the information security and product development / engineering organizations to work closely together, as well as having the right skillsets.

Similarly, as organizations embrace cloud computing, mobility, leverage APIs, Artificial Intelligence, software defined networks and other digital advancements and technologies, security risks and approaches have to be thought through and proactively built in and applied e.g. configuration controls are critical for Infrastructure as a Service. This cannot be done well if the security teams do not fully understand the concepts and nuances of the technologies, and realize that while underlying principles remain the same, different approaches need to be deployed to meet security objectives.

Supply Chain

Supply chains continue to be an avenue of attack. This can manifest itself in several ways. Attacks might compromise and plant malware into software products and components that are widely used. Attackers might also infiltrate organizations aka third parties e.g. managed service providers, who provide services to corporations and then use that access to launch attacks against other organizations. Reuters reported in Dec 2018 that several large managed service providers (MSPs) were hacked and their clients were then attacked.

Organizations thus should have third party risk management processes in place to address aspects like vendor due diligence, security language in contracts that require adherence to security standards and audits, and ongoing monitoring of supplier security where appropriate. An organization should also remember that it cannot outsource its accountability for security – a common misconception in using cloud services. Conversely, if an organization is a supplier, it should to attuned to the risk that it might be targeted just for these purposes, and tune its security strategy and defenses accordingly.

Cyber Insurance

Cyber Insurance is an increasingly important way organizations can manage some of their risks. There can be nuances in coverage of cyber insurance, particularly on how specific attacks like ransomware, business email compromise (BEC) scams are covered i.e. coverage might be under a general fraud section as opposed to cybersecurity. Thus it is critical to fully understand how coverages will play out in different scenarios.

The Interplay of Security and Privacy

Privacy regulations are sweeping the world and while the impact will vary depending on an organizations business model and

global footprint, there undoubtedly will be an impact for most organizations. While Security and Privacy are sometimes used synonymously, they are different concepts. Privacy regulations are generally centered around providing individuals control and rights over their personal data, and ensuring principles of transparency, protection and fairness and followed by organizations that collect and use it. Protection of data is undoubtedly one of the key objectives where there are synergies between security and privacy, as well as objectives on data minimization. It is imperative to meet privacy regulations, that an organization identify and map where its personal data is, understand the data flows etc, all of which will have the effort of the organization reducing data sprawl and redundant copies of data- thus reducing information security risks as well.

Conclusion

Cyber security can seem like a daunting and insurmountable problem which is just going to get worse. And it is true that the risks are increasing and that solving the broader problem requires solutions from governments, regulators, industry groups and political leaders and not just organizations. But having said that, organizations can take concrete steps to manage their cyber risks. By ensuring they have the right security capabilities, building a business focused and supported information security program which brings clarity and relevance of those risks in the context of the organization, driving a culture of security and risk management across the organization, and ensuring the basics hygiene practices are addressed, most organizations can significantly enhance that their defenses and capability to address a broad range of cyber threats, and thus minimize the impact and disruption to their business.

References:

www.zdnet.com/article/credential-stuffing-attacks-cause-heartache-for-the-financial-sector/
www.bankinfosecurity.com/yahoo-takes-350-million-hit-in-verizon-deal-a-9736
www.news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/
www.usatoday.com/story/money/2018/01/14/car-hacking-remains-very-real-threat-autos-become-ever-more-loaded-tech/1032951001/
www.securingtomorrow.mcafee.com/other-blogs/mcafee-labs/todays-connected-cars-vulnerable-hacking-malware/
www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html
www.arstechnica.com/information-technology/2017/08/465k-patients-need-a-firmware-update-to-prevent-serious-pacemaker-hacks/
www.telegraph.co.uk/travel/news/hotel-key-cards-safety-hack/
www.reuters.com/article/us-china-cyber-hpe-ibm-exclusive/exclusive-china-hacked-hpe-ibm-and-then-attacked-clients-sources-idUSKCN1OJ2OY
www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/

6

Essential Behavioural Competencies Required to Manage the Next Generation of Cyber Risks

HDFC Bank - Sameer Ratolikar,
Executive Vice President & CISO

With the growing complexity in technological trends, digital revolution cyber security risks have taken a different shape. While innovation is happening in cyber security risk management we unfalteringly need new age cyber security skill sets. It is not plain selling to get these skill sets from open market. To my mind, if we select talents with sound behaviour competencies, analytical abilities, inter personal skills and personality traits they would be able to learn and adapt themselves into new age cyber security specialists.

Some of the important behavioural competencies generally I look for cyber security defense and risk management areas are:

Curiosity

Inquisitive minds with strong intellectual curiosity plays a very important role in the team. Cyber security is a dynamic area which requires continuous learning, researching, listening attentively, constantly absorbing and infusing learnings in further refining the initiatives. I have seen many times business teams consult the information security team to seek an advice on various digital initiatives. In such situations, people with a curious minds can generate various options to help the business teams. It is important that the team members be advised to attend webinars, conferences to learn and imbibe their learnings in the work. There are various areas in cyber security right from basic hygiene initiatives like patch management to vulnerability management, AI/ML based trends, dark web monitoring and shadow IT. In all these pertinent areas, curiosity and enthusiasm would be helpful to boost the curve.

Adaptability

The cyber champs these days don't want a traditional work culture, rather they would prefer a bring your own device (BYOD) type of concept, flexible office tim-

ings and jazzy work place design. Change in the leadership, technology, work place and organisation at times creates a kind of different vibes among the team members. So, it is very important that the team members adjusts to the new boss, senior team and more importantly to the work place. It is very important for a CISO to regularly interact, engage with them to convey positive feeling about the new organisation. Other important aspects are change in the leadership/boss, technology tools and processes. Often these things create uncertainty about their future and hence pessimism among the team mates. Continuous dialogue, encouragement, challenging and satisfying work often helps to make new guys comfortable and adaptable.

Self confidence

Self confidence among the team members is very crucial especially in a situation of cyber crisis. The threat landscape is evolving at a rapid pace and "fear of the unknown" will always remain. Having a firm belief in the thoughts, actions and capabilities during the cyber crisis create a conduit for smooth crisis management. Having self-confident members in a team create a positive motivation in others. This allows for team members to be creating and come up with good ideas whilst confidently handling tasks without waiting for consultants to provide all the advice.

Enthusiasm

Having a sound design/policy framework is one aspect but strong timely, effective and monitoring the effectiveness of the security controls is extremely important. It is very important that the team members maintains consistent level of productivity, enthusiasm and delivery based outcome. Regulatory mandates and remediating high risk vulnerabilities requires vigour, pace and taxing work. There could be times especially in a situation of cyber security incidents and crisis where team members may be required to work for extended hours and hence enthusiasm and exuberance becomes indispensable.

Loyalty

Even though the cyber security strategy is formulated to include a criteria for zero tolerance, in practice there are situations where trust plays a very important role. Whatever security solutions are deployed and with the dynamic threat landscape, experience shows that no solutions are 100% effective and there are certain residual issues. Keeping the trade secrets, critical controls, policies, network blueprints confidential is an essential aspect for cyber security investments and strategies. Make sure that the loyalty aspect is reiterated on a regular basis so that team members knows the seriousness of adherence and consequence of breaching it.

Open mindedness

At times, I have seen team members be closed minded on certain areas for example – cloud, open banking, 3rd party engagements etc. But, with the changing shift in the consumer demands, progressive regulation and digital disruption there has to be a balance between the security and business. More importantly, I have always believed in the CISO's approach to be more of a business enabler and manage the risk with innovative ideas and approaches. Having open mindedness among team members is a cardinal aspect to ensure that they enable the business. Another aspect is not get disheartened by certain transactional failures be it cyber security incidents, non-cooperative business teams. Try and incorporate the feedback, suggestions to make further inroads in the organisation and create visibility. Visibility is a key of success for CISO and his team.

Ownership

One of the important aspects of making a cyber security programme effective is to see that there exists an ownership within the organisation. Cyber security risks lies within the technology function, with 3rd parties and with different business processes. It is extremely important for a CISO and his team to own these risks and get them mitigated and ensure

proper communication and engagement with the stakeholders. The engagement should focus on explaining the stakeholders the evolution of cyber security risk as business risk with strong data points, incidents manifested, growth in the vulnerabilities, RED team results. Data should speak. Once the CISO owns the cyber security risk across an enterprise I believe, it gives him a great amount of visibility and a chance to take the function to a strategic level and be a part of the board room discussion. Remember, there is only one CISO/ information risk manager so the role has to be powerful and empowered.

Resilence

There is nothing like 100% cyber security. We can only harden the layers and make the attackers job difficult. In case of cyber crisis it is paramount to remain calm, follow the plan and handle the crisis. A "don't give up" attitude is extremely helpful in such situation. A team who think long term and identifies the critical risks, prepare contingency plans, test the plan through table top exercises and simulation drills will be better prepared and be more resilient.

Delivery focussed orientation

Having a comprehensive policy framework is one aspect, but if execution doesn't happen within the timelines it can have a big impact on the effectiveness in cyber security. It is critical to mitigate the risk in a timely manner irrespective of the operational challenges. The fact that the information security team has to depend upon many stakeholders to reduce the risk and hence the teams having delivery/ result focussed orientation is essential. The progress in the delivery must be tracked by the CISO periodically and actions must be taken to correct anomalies, if any. In achieving the objectives, the team members might need adequate resources, budgets which need to be provided to them.

Ambitious

Ambitious team members must have a strong desire to achieve the targets, whether it's a milestone or to achieve success through their efforts. They need to be persistent and determined. If their work is getting affected by major/ minor issues they need to step up to the challenge to do everything to sort out the issues.. If there are any setbacks, they need to learn in order to grow and improve. If there are any learning opportunities, ambitious team members will put themselves ahead and focus on growth.

Proactive

Taking up new initiatives into consideration of the cyber security goals without being forced is an example of a powerful team. Self-supervision and disciplined of team members is the key. In my career, I have seen certain team members who are ready to take up the tasks which others have either not taken up or not too keen to take up. Anticipating the threats, planning and taking up the counter measures is very crucial to manage the complexity in the cyber space.

Effective communication

Many times as part of the risk management especially arising out of 3rd party vendors, requires effective communication on the risks at hand without getting into great technical detail. Business leaders need to understand the risk to the business in plain English. The impact and what is at stake to them needs to be clearly articulated. The risk likelihood and how it impacts their day to day business should be clearly expressed. At this level, effective communication is very essential to bring them on-board. Often, complex technical jargon used during a presentation becomes an obstacle in achieving the end objective. If the team lead is able to explain the business impact of the risk, incidents manifested and sophistication of the attackers my experience has shown that business leaders understand it very well and risk reduction becomes seamless.

Teamwork

Once the goal is set, collaboration among the team members plays a very important role to effectively execute the cyber securi-

ty initiatives. At times, there could be some overlapping activities depending upon the roles and responsibilities created within the team members and hence team work to achieve the common goal is very crucial.

7

Cybersecurity: Need for a Holistic View

Indian Institute of Information Technology, Bangalore (IIIT-B) - Professor S. Sadagopan, Director

Cybersecurity issues are not new. However, lately there has been a lot of buzz around this topic.

This is not surprising, considering that while for a long time cybersecurity issues impacted only hundreds or at the most thousands, of people, now the dramatic "digital" transformation of society has made billions of people—practically the entire human race—vulnerable.

Reports of someone making an ATM dish out currency from another person's account, the privacy of account holders in a bank being compromised, a cloud provider sending a sorry note to a million customers, requesting them to change their passwords because their passwords have been hacked, and even a car odometer being re-set from the network by a person other than the owner, have become common.

Naturally, there is panic, fear and unease in the minds of common people regarding the security of the information stored by banks, network providers, universities and government agencies.

True, There Are Problems

While industry folk try to assuage the fear, and talk of multiple solutions like virus protection software, encryption schemes, intrusion detection systems, and firewalls, it cannot be denied that system administrators are finding it difficult to cope with large pieces of protection equipment, both in terms of investment and operating costs.

Industry leaders often complain to universities about the shortage of trained manpower.

Industry associations (armed with consultants who make "quick & dirty" estimates) lobby with governments to create funds to "train" and "re-train" lots of people who can take up the new positions of "cybersecurity professionals".

Meanwhile, governments are busy setting up task forces to advise them on what their "strategic response" should be.

Digitalization Leaves No One Untouched

It is undeniable that cybersecurity will need to be ubiquitous. This is because digitalization, being a game changer, is impacting all professions – banking & finance, manufacturing, logistics, transportation, oil & gas, government, education and healthcare, to name a few. The benefits that dititalization brings, are catalyzing its adoption by various sectors.

Online course delivery, libraries and publishing are changing the face of education fundamentally. Robotic surgery and AI-assisted doctors are starting to change healthcare in a fundamental way.

E-commerce has changed the very notion of retailing. Digital technology is dramatically changing banking, stock trading, insurance and financial services.

Ticketing is moving to near-100% electronic form. Travel, hospitality and entertainment are impacted too; Uber and Airbnb are re-inventing taxi aggregation and hotel room aggregation respectively; similar developments are happening in music, video and movie delivery.

Fly-by-wire is maturing and driverless cars and drones are under intense development, with deep impacts on the transportation industry. Governments are embracing digitalization, promoting e-delivery of citizen-centric services.

When all industry segments move to "digital", cybersecurity issues are inevitable, and it is obvious that most civilians will be impacted by these issues.

Some dramatic cybersecurity incidents have led to panic reactions. One example in the recent past was the admission by Facebook that the personal data of millions of users was compromised. This resulted in loss of market value of $ 13 billion in a day as the disclosure sent shock waves across the tech industry. Another is of an ATM network getting "hacked", leading to panic among millions of retail consumers, which, in turn spooked financial systems' regulators.

Will Affect Military Might

While this is the situation on the civilian front, the impact on the military forces will be even more pronounced. Consider this: thousands of years back, the power of an army was measured by the number of men in it, and the number of animals—mostly horses—they controlled. Hundreds of years later, after the invention of cannons and guns, the power of the armed forces started to tilt towards "strike power" measured by machinery. Today, the parameters for measuring the power of an army are completely different, thanks to the introduction of tanks, war planes and warships (including submarines). In the years to come, all the main "gears" – tanks, planes and ships will be networked, controlled by software, and controllable remotely over the network.

Desperate armies try to create panic through civilian damage. Armed forces can, in the future, impact financial networks, power networks, transportation networks and government networks in ways unprecedented in human history, thanks to advances in computing, communication and control technologies (including machine intelligence). The strength of tomorrow's armies will be measured by networking and software capabilities, in addition to physical prowess.

Naturally, cybersecurity will play a decisive role in the evolution of military forces in the future.

Cybersecurity over the decades

While cybersecurity issues are not new, they have now become important enough to be discussed at the global level.

Due to the surge in Internet usage and the exponential increase in data networks, data network security vendors have over the past couple of decades developed amazing tools and techniques to manage end-to-end security. Among these are virus protection software, intrusion detection and firewalls.

The telecom industry which is over a hundred years old, has also developed sturdy security tools.

Post-1995, the exponential growth of mobile networks and backhaul networks (terrestrial cables, fiber optic networks, submarine cables and satellites) on one hand, and the dramatic change in end-user expectation on the other (fueled by tools like Facebook and WhatsApp), have complicated life.

Billions of end-users who started accessing the complex network often through mobile devices, and the "millennials" using networks in a fundamentally different way, have led to a situation where the boundaries between creators of data and consumers of data are blurring.

Governments have not been given sufficient time to frame the right regulation.

In this "mismatch scenario" many bright individuals and groups have been able to create havoc among "unsuspecting" end-users. An unusual phrase, "ethical hacking", has become part of common parlance.

An interesting fact, often not known to people outside the community of core voice and data network experts, is that the industry developed on "trust", "openness" and "cooperation". For example, practically every network server "routes" e-mails directed to a remote client. Such "open systems" create "global public good" of tremendous value; unfortunately, they can also be misused by people with very different values.

In today's world, where cybersecurity issues are in the spotlight, sufficient capability will surely be built to address all the security issues. It will take some time, but there is no need to panic.

Lessons From Fire Safety

When electricity was introduced in homes and offices, it threw up multiple challenges, the most important being the chance of houses catching fire (primarily due to short-circuiting). Fire safety became even more important with architects using false ceilings, wood, and polyester-based partitions that are inflammable .

No doubt, there were several nasty accidents both in homes and offices, but over the years systems were developed to improve fire protection. For example, fire hydrants in the form of fire cylinders that can put out fire evolved; later, fire-hydrant-based sprinkler systems with sophisticated controls and specialized chemicals to put out fires real fast were developed. Additionally, building contractors were required to incorporate fire safety into the building design. Professional societies that regulate construction professionals got the techniques codified in the form of "building codes". In turn, municipal governments that are charged with civilian safety got such building codes incorporated into laws; legislation included punishments for violation.

A sophisticated system of fire safety, involving fire inspectors, fire engines and a toll-free number to report fire were developed over the past two centuries. All this has ensured that we all can sleep peacefully in apartments, work in offices, shop in malls, and watch movies in cinema halls without worrying unduly about fire.

The sophisticated interplay of technology, professional practices, fire safety laws, and law enforcement machinery gives us this comfort.

Consider this: a city like Bengaluru, with a population of more than ten million, has just a few hundred firemen, and most fires in the past decade have been handled well.

Cybersecurity will be no different.

It will just take a little time to evolve. However, while fire safety evolved over decades, cybersecurity will mature in just over a decade. Sophisticated tools and techniques will evolve, the technical knowledge to support such tools will come out of universities and government / industry R&D labs, and specialized training courses will be developed. The bottom-line, however, will be that the number of cybersecurity professionals will be in thousands or possibly tens of thousands, but not in millions!

However, millions will be cybersecurity literate—just as every office employee / dormitory resident goes through a compulsory fire drill as a safety measure. Schools and

colleges now sensitize students to fire safety; tomorrow's students will be sensitized to challenges related to cybersecurity. In short, it will be a part of citizen education.

8

Securing Cyberspace is Key to Success in the Digital Age

KPIT Technologies - Mandar Marulkar, Chief Digital Officer

In the digital age, technologies such as cloud, IoT (Internet of Things) and M2M (machine-to-machine connectivity) are visibly disrupting enterprises with new business models, differentiated customer experiences, optimised processes and improved productivity. The underlying aim of such disruptions is to make people productive by giving them access to the right insights at any point in time.

As digital technologies are accelerating the pace of innovation, it is helping us to collaborate not only with people but also with things in a trusted manner, leveraging data creatively and freely through technology. As we use more and more technology in every aspect of our life, Trust on the technology and people has increased exponentially. For e.g. going forward as we get into autonomous driving, we strongly accept the relationship between trust and innovation. Everything a person does in that commute is underpinned by trust: we trust a car to run as per the specified route safely. When we get into smart home, we expect our coffee machine not to mess up with our preferences. Similarly when we do any transaction online, we trust our data reaches to legitimate site to ensure a confidential transaction is not uploaded to a rogue phishing website. And, since trust is established between parties, customers, suppliers, financial institutes, logistics companies, we expect everyone's role to protect critical data at all times.

Trusted interactions lead to the creation of value for a company, but the intersection between end-user and data is also the point of greatest vulnerability for an enterprise, and the primary source of breaches driving cyber risk to all-time highs. How can security professionals know if an end-user login is the result of an employee's open hotel WiFi access or an attacker abusing authorized credentials? How do we know whether a user identity is behaving consistently or erratically on the network compared to an established routine? Knowing and acting on the difference between an indi-

vidual legitimately trying to get their job done and a compromised identity is the difference between innovation and intellectual property (IP) loss, the difference between an organization's success or failure.

As data and digital experiences are placed into the hands of others, the concept of trust becomes even more crucial. Businesses can rise or fall based on trust. We have seen many disasters like a breach of personal data, hacking of websites and so on in the cyber-space since the start of the 21st century. We know that nation-states are behind the worst digital attacks against both innocent people and the infrastructure that underpins societies – energy, transportation, health care, financial, food and water. Virtually every digital attack ripples beyond its intended target and harms the lives of innocent citizens.

For example, the 2017 "WannaCry" attack – a true wake-up call – tore through cyberspace, hijacking more than 300,000 computers across 150 countries, including computers used by families, hospitals, governments and businesses. WannaCry was followed closely by "NotPetya," an attack estimated to have caused $10 billion* in damage ranging far beyond the initial targets in Ukraine. WannaCry and NotPetya were our wake-up moments; they raised an alarm: if we don't act now, global cyberattacks will continue to inflict grave economic harm and risk human lives and well-being.

In India, daring cyber-attacks was carried in August 2018 on Cosmos Bank's Pune branch which saw nearly 94 Crores rupees being siphoned off. Hackers wiped out money and transferred it to a Hong Kong situated bank by hacking the server of Cosmos Bank. The attack was not on centralized banking solution of Cosmos bank. The switching system which acts as an interacting module between the payment gateways and the bank's centralized banking solution was attacked. This was the first malware attack in India against the switching system which broke the communication between the payment gateway and the bank

There are many types of cyber attacks, however some of the common types are

Denial-of-service (DoS) and Distributed denial of-service (DDoS) attacks

A denial-of-service attack overwhelms a system's resources so that it cannot respond to service requests. A DDoS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker. Unlike attacks that are designed to enable the attacker to gain or increase access, denial-of-service doesn't provide direct benefits for attackers. For some of them, it's enough to have the satisfaction of service denial. However, if the attacked resource belongs to a business competitor, then the benefit to the attacker may be real enough. Another purpose of a DoS attack can be to take a system offline so that a different kind of attack can be launched.

Botnets are the millions of systems infected with malware under hacker control in order to carry out DDoS attacks. These bots or zombie systems are used to carry out attacks against the target systems, often overwhelming the target system's bandwidth and processing capabilities. These DDoS attacks are difficult to trace because botnets are located in differing geographic locations

Man-in-the-middle (MitM) attack

A MitM attack occurs when a hacker inserts itself between the communications of a client and a server. Like in case of Session hijacking, an attacker hijacks a session between a trusted client and network server. The attacking computer substitutes its IP address for the trusted client while the server continues the session, believing it is communicating with the client.

Phishing and spear phishing attacks

Phishing attack is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do some-

thing. It combines social engineering and technical trickery. It could involve an attachment to an email that loads malware onto your computer. It could also be a link to an illegitimate website that can trick you into downloading malware or handing over your personal information.

Spear phishing is a very targeted type of phishing activity. Attackers take the time to conduct research into targets and create messages that are personal and relevant. Because of this, spear phishing can be very hard to identify and even harder to defend against. One of the simplest ways that a hacker can conduct a spear phishing attack is email spoofing, which is when the information in the "From" section of the email is falsified, making it appear as if it is coming from someone you know, such as your management or your partner company. Another technique that scammers use to add credibility to their story is website cloning. They copy legitimate websites to fool you into entering personally identifiable information (PII) or login credentials.

Drive-by attack

Drive-by download attacks are a common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. This script might install malware directly onto the computer of someone who visits the site, or it might re-direct the victim to a site controlled by the hackers. Drive-by downloads can happen when visiting a website or viewing an email message or a pop-up window. Unlike many other types of cyber security attacks, a drive-by doesn't rely on a user to do anything to actively enable the attack, you don't have to click a download button or open a malicious email attachment to become infected. A drive-by download can take advantage of an app, operating system or web browser that contains security flaws due to unsuccessful updates or lack of update.

There are many other types of attacks like SQL injection, Cross site scripting, Eavesdropping and malware attack. Ransomware is one of the common malware these days. Ransomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid. Some advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files in a way that makes them nearly impossible to recover without the decryption key.

Majority of the cyber-attacks resulted in financial damages for the companies. It is not a surprise that cybersecurity and data security have become a necessity more than ever before. A few years back, spending on cyber security was the last priority for Indian companies. However, today it has become the top priority and the chief Information security officer (CISO) plays one of the most crucial roles in the company. The role of the CISO becomes even more critical as it is predicted that by 2021, the annual damage caused due to cyber crimes would sum up to around USD 6 trillion.

Cyberattacks are typically termed as confidentiality (data which is stolen), integrity (data which is manipulated to encrypted by a 3rd party) and availability (preventing you from accessing infrastructure and applications) issues. It calls for the stakeholders to share the responsibility of securing the cyber-space to ensure the safety of the data and information.

Attacks nowadays are sophisticated, automated and machine-driven rather than human-led, majority of which are carried out with the intention of making money fraudulently. Also, currencies, such as the Bitcoin have created a parallel financial ecosystem, helping attackers to make money and build a multi-million dollar industry in the last ten years.

It is not an exaggeration to say that cyber-attacks even have the potential to trigger a world war. For instance, it is virtually possible for a country to use the botnet network of another to generate an attack on a third nation with minimal chances of getting exposed.

Wiring the cybersecurity framework

There are two types of security issues that organisations should make a note of—information-security and cyber-security. Information security involves securing the trusted infrastructure, including the servers, networks, the company managed in-points and so on, with firewalls, end-point security solutions, web content filtering solutions and intrusion prevention solutions. Cyber-security entails protecting the many devices, such as sensors-installed home appliances, cars, gaming stations and smart factories that connect the world to the Internet.

Network deployments have significantly changed over the past decade. Businesses are rapidly moving to the cloud and adopting new technologies such as Internet of Things (IoT) and block chain, all of which are heavily dependent on the network. These same enterprises are also increasing spending on security to protect new and existing infrastructure, but the breaches continue unabated. Internal records and customer information are still being stolen and sold to the highest bidder, causing irreparable damage to corporate reputations. Key stakeholders are faced with the realization that their considerable investments in popular security products have still not yielded the promised protection. This is because typical infrastructure and security products have the following issues:

- **Uncoordinated and Firewall focused:** Firewalls preventing the client from reaching outside the corporate network are ineffective and do not protect against lateral threat propagation.
- **Complex security policies:** Companies require providing access to various applications, users, devices using dynamic ports making it complex to setup policies. Also, companies find it difficult to whitelist/blacklist set of applications/ user traffic making it more complex.
- Typical endpoint security solutions are still focused on signature based technologies to protect against known viruses making it ineffective for advance malwares and day1 attacks.
- **Limited Visibility:** The inability of security solutions to communicate with, and leverage networking components reduces visibility and restricts the number of enforcement points.
- **Lateral Threat Propagation:** Failure to aggregate reports of abnormal behavior from different knowledge sources such as logging servers, endpoints, and other network elements is a significant weakness in security strategy.
- Since the security strategy is heavily firewall focused, the complexity of firewall policies can easily overwhelm security teams; this problem is amplified when the enterprise has global footprint.

Though nowadays, attacks are generated by smart machines (programs/algorithms powered by artificial intelligence), enterprises still depend on people to protect and prevent them from such attacks, which leads to a fundamental difference or gap in the approach. Enterprises are implementing their digital transformation initiatives using an architecture that is suitable only for information security and not cyber-security. In my opinion, there is a high possibility that the hackers will start attacking unmanaged new end-points unless one has a relook at the complete cyber-security architecture.

With the goal of monitoring and analyzing network activity to detect and defeat cybersecurity threats and other anomalies, the security operations center(SOC) represents the first line of defense for any organization. SOC analysts perform tasks like log monitoring, incident response, compliance, penetration and vulnerability testing, key and access management, and so on… However it can take years of experience to develop competency in implementing effective security operations. These diverse functions also often run on numerous disconnected systems, leaving analysts to deal with countless streams of data and alert feeds that can overwhelm even the most weathered security practitioner. Analysts desire for a “single pane of glass” solution,

one place where all the tasks they have to deal with show up with the context and timeliness they need to prioritize their work.

Threat intelligence is essential for making this picture a reality. Good threat intelligence provides exactly the context needed to enrich data feeds, reduce alert fatigue, and help SOC analysts work more efficiently and make informed decisions.

To assist security professionals (SOC), companies need to deploy new age security analytics solutions which extensively use machine learning. Such solutions require humans to upload new training datasets and expert knowledge. Typically we need to provide logs and context caputured by various network, data center, cloud applications and end point devices as high quality input. Machine learning provides clear advantages in outlier detection, much to the benefit of security analytics and SOC operations. Unlike humans, machines can handle billions of security events in a single day, providing clarity around a system's "baseline" or "normal" activity and flagging anything unusual for human review. Analysts can then pinpoint threats sooner through correlation, pattern matching, and anomaly detection. While it may take a SOC analyst several hours to identify a single security alert, a machine can do it in seconds and continue even after business hours.

However, as on today, most of these security analytics solutions are new and not really matured. We cannot rely too heavily on these technologies without understanding the risks involved. Algorithms can miss attacks if training information has not been thoroughly scrubbed of anomalous data points and the bias introduced by the environment from which it was collected. In addition, certain algorithms may be too complex to understand what is driving a specific set of anomalies.

In addition to focusing on proactive monitoring, Enterprises need to set up a prevention-based architecture and not just detection and response-based ones. However, if an attack is detected in the infrastructure, one should be able to isolate it and restore the services as quickly as possible. As a part of new cyber security architecture, organsiations should focus on

a. Accurate Threat Detection for Known threats as well as Unknown threats. For Known Threats, companies should consolidate threat information from inhouse logging, cloud feeds (Command and control, Geo IP) and Third party via REST API. For Unknown Threats, companies should look at solutions providing Sandboxing, machine learning and deception.
b. Centralized Policy and Analytics: Visibility into every corner of the endpoint, network, application irrespective of whether data at rest or in motion and stored on premise or on cloud. Unified Security policies and management from the centralized single pane of glass.
c. Dynamic Automated Policy Enforcement: Leverage every endpoint (server, end user device like desktop/laptop, smart phone, network devices, IoT gateways) as enforcement point. Facilitate rapid and automated threat intelligence. Ensure that East West as well as North-South traffic is secured. End-point detection and response (EDR), network behaviour anomaly detection and user behaviour analytics solutions can be used to identify suspicious activity happening in the device, track its source and protect the infrastructure by configuring the appropriate policies. Such solutions typically baseline the normal behaviour of the device or application and look for abnormal behaviour due to advanced malware or vulnerabilities in the system.

Another important aspect is to have the outside-in intelligence on a real-time basis right from the beginning. Enterprises should have the capabilities to prevent their infrastructure from any attacks and threats whose origin or effect is seen in other countries and industries as well. And, that is where multiple intelligence of the cloud comes into the picture. They should be integrated with on-premise next-generation firewalls that auto-

matically prevent the threat and are updated or configured into the enterprise's next-generation firewall without any human intervention. If any new threat is detected, the infrastructure should update even without the involvement of a security operation team member. Organisations should not only look at protecting data and apps from their private cloud, but also from public cloud SaaS (software-as-a-service) applications, servers or cloud-based data repositories. Advanced malware, secure authentication and data-leak prevention technologies need to be implemented for public cloud applications and data repositories.

Trends in Endpoint security

Endpoint security is focused on locking down endpoints - individual computers, phones, tablets and other network enabled devices in order to keep networks safe.

The end point security measures run on two tiers: there are software agents that run in the background on endpoints, and a centralized endpoint security management system that monitors and controls the agents. That management system can be a control panel monitored by IT staff or an automated system or some combination of the two.

Now a days, endpoint protection solution covers device security functionality into a single product that delivers antivirus, anti-spyware, personal firewall, application control and other styles of host intrusion prevention (for example, behavioral blocking) capabilities into a single and cohesive solution.

Traditionally definition of an end point was always a computer, whether it is a desktop or laptop. In the past, computers were connected to internet typcially in the office environment and most of the computers at home were used in stand alone. As the penetration of internet has increased in India including rural ares, most of the computers are always connected on network. In additon to computers, most of the transactions are done over smart devices whether it is Smart phones or tablets. They are typically connected on cellular data network or wireless connection over home broadband or office network. As we started embracing digital technologies in all parts of our life, we have now smart homes, Smart factories, Smart campuses, Smart mobility making every device connected over internet by use of IoT embedded in various devices. Of course, as threats evolve, endpoint security suites must evolve as well.

- **Machine learning**. As threats accelerate and primary threat source is a machine (Smart program written by intellient hackers) it is too much, too fast for any human to keep up with in real time. Traditional way to deplomen of security updates and signature based technolgoies are becoming ineffective. Endpoint security manageemnt is increasingly automated, with machine learning examining traffic and identifying threats, and only the most pressing needs being escalated to human attention.

- **SaaS-based endpoint security**. As organisations started adopting cloud solutions for mission critical business services like Email, ERP, CRM etc. they have also started focusing on using more and more SaaS soltuions in the infrastrucutre area to reduce management overheads and keeping updated with the technology innovations. Traditionally, centralized endpoint security management systems run on a server or appliance that an organization deploys and cares for in-house. But with cloud- or SaaS-based services becoming increasingly trusted as part of IT's day-to-day operations. Many companies have started taking endpoint security management as a service from leading security vendors. In some ways, this is not unlike the move to machine learning, companies are offloading responsibility for managing endpoint security away from their own internal employees and of course many of these SaaS services are using machine learning behind the scenes as well.

- **Layered protection against fileless attacks.** Fileless attacks, which are perpe-

trated by malware that resides entirely in RAM and is never written to disk, is an attack vector growing at an alarming rate. Typcial signature based technolgies doen't help in protecting endpoints from such threats. Endpoint security vendors are rushing to provide the layered defense necessary against this type of attack. Often it's necessary to combine this with automation and machine learning, as current tools can generate a number of false positives, and chasing them down will consume precious IT resources.

- **Putting IoT devices under the protective umbrella.** One of the big stories of internet security over the past few years is that literally billions of internet-connected "things" - cameras, sensors, routers, are out doing doing jobs quietly without the protection. For an example, look no further than the Mirai botnet, which college students created by hijacking thousands of closed-circuit TV cameras to launch DDoS attacks against rival Minecraft server hosts, accidentally launching some of the biggest denial of service attacks ever recorded. Mirai is a self-propagating botnet virus. The source code for Mirai was made publicly available by the author after a successful and well publicized attack on the Krebbs Web site. Since then the source code has been built and used by many others to launch attacks on internet infrastructure. The Mirai botnet code infects poorly protected internet devices by using telnet to find those that are still using their factory default username and password. The effectiveness of Mirai is due to its ability to infect tens of thousands of these insecure devices and coordinate them to mount a DDOS attack against a chosen victim. While many IoT devices are running bespoke OSes that are difficult to manage, the majority are running Linux, iOS, Android, or even Windows variants, and endpoint management vendors are starting to develop software agents that can run on them and bring them in from the cold.

- **Reducing complexity and consolidating agents.** As the market segment has grown, many endpoint security vendors have offered a proliferating and confusing array of tools, each targeting a specific kind of attack or vulnerability. The upshot is that companies have as many as seven different software agents running on each endpoint, each of which needs to be managed separately. However, most of the secuirity vendors are aiming to unify their offerings into consolidated suites and include most of the functionality into the single agent managed centrally from the cloud.

Even if the endpont security solutions are enhanced substantially, they still have many challenges. Most of these solutions still require separate end point functionlity for information protection like Data leak prevention or device control. Also many solutions give false alarms and lack of automation increases management overhead making then ineffective in deployment.

Security risks in Industrial IoT

With the pervasive adoption of connected devices as integral part of digital applications, the notion of Internet of Things (IoT) is now a key consideration of cyber application designers and business solution planners. The scope of cybersecurity has evolved as well to include not only traditional IT systems but also OT systems and more recently IoT systems. Nevertheless, as a fast developing and promising area in the future landscape of Industry 4.0 applications, but with limited prior experiences in the adoption and security protection strategies, IoT security remains a challenge to digital practitioners. The issues include, the adoption strategy of IoT in digital applications, the business process integration of IoT, the development of security policies that are relevant to IoT adaptation and security architecture that caters to the needs of IoT security.

The security of the IoT is a concern not only for the wearable devices that most people associate with connected devices,

but also for the critical information infrastructure on which we all depend. The IoT will soon become the biggest attack vector for most organisations, as the number of connected devices is set to grow explosively. Nowadays, companies recognise the value of the IoT, but most find it difficult to integrate into their current business processes and struggle to process the massive amount of heterogeneous data being collected. Companies have not adequately addressed the risks associated with the collection of data from various sensors. Most of the companies who are embarking on the IoT journey are worried about security architecture and cybersecurity incident response processes.

Networked industrial control systems (ICS) that require "always-on" connectivity represent an expanded attack surface, and nowhere is that more apparent than in IoT devices. WiFi and other network connected sensors in autonomous vehicles and appliances have introduced a rapidly evolving set of security requirements. While attacks on consumer IoT are prevalent, the possibility of disruption in manufacturing and similar industries makes the threat all the more serious. There is high potential for man-in-the-middle (MITM) attacks on IoT networks. Attackers can break into industrial IoT devices by attacking the underlying cloud infrastructure. This target is more desirable for an attacker who can get access to the underlying systems of these multi-tenanted, multi-customer environments. We need to understand three key issues

1. Increasing network connectivity to edge computing,
2. Difficulty in securing devices as more compute moves out to the edge, as they do in remote facilities and IoT devices,
3. And the exponential number of devices connecting to the cloud for updates and maintenance.

Attackers seek out vulnerabilities in cloud infrastructure which IIoT devices uses at scale. As control systems continue to evolve, they will be patched, maintained, and managed via cloud service providers. These cloud service providers rely on shared infrastructure, platforms, and applications in order to deliver scalable services to IoT systems. The underlying components of the infrastructure may not offer strong enough isolation for a multi-tenant architecture or multi-customer applications, which can lead to shared technology vulnerabilities. In the case of industrial IoT, a compromise of back-end servers will inevitably cause widespread service outages and bring vital systems to halt. Manufacturing, energy production, and other vital sectors could be affected simultaneously.

In 2018, we saw Meltdown and Spectre exposing vulnerabilities in modern computers leaking passwords and sensitive data. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents. As Meltdown and Spectre work on computers, mobile devices, and in the cloud, depending on the cloud provider's infrastructure, it might be possible to steal data from other customers as well. It can bypass the software and firmware layers to expose processor hardware to exploits. In this scenario, attackers can use low-privilege programs in order to access more critical data, such as private files or passwords. Almost all CPUs since 1995 are thought to be vulnerable, 12 and new variants of Spectre continue to surface. Attackers will divert their attention on developing variants that subvert the underlying cloud infrastructure used by IIoT systems. As processor speed is critical to performance, manufacturers and cloud service providers could

continue to choose speed over security in order to gain a competitive edge, inadvertently introducing further vulnerabilities. Organizations will need to move from visibility to control where the IT and OT networks converge to protect against these deliberate, targeted attacks on IIoT systems. IoT will be the most challenging area of security. Not many security professionals have had time to focus on IoT and it is becoming the trend in our life. It's consistently getting bigger and bigger, and it can be very dangerous when IoT devices get exploited.

Cybersecurity culture

Today when any customer offers work to any company or signs partnership, they typically do significant due diligence based on security requirements and compliance with laws and industry standards. Customer wanted to know whether the work outsourced to partner has sufficient security infrastructure and culture to protect intellectual property. Today, in cloud-first, mobile-driven users and data roam freely on networks, leaving critical data and intellectual property more exposed than ever. Customers are more and more doing the due diligence on how much trust they can put into the security of a partner.

Security cannot just be the responsibility of the IT teams and the technologies they implement, but must become a cultural and business value that is recognized and rewarded. To build a workforce united as a defense against cybercrime, organizations must integrate security into their culture from the top down.

Culture is collective behavior of people and includes not only employees but also the partner ecosystem. Security Culture includes much more than the organization's values, policies and processes and authorization matrix. It also includes the chain of command, delegation of authority, accountability for behaviors, and broad communication strategies. Policies that are ill-defined or in conflict with one another create confusion and misinterpretation. Any confusion regarding rules, expectations, or accountability can increase risk, including risk of a data breach.

Companies need to invest time and money in continuous educating all the stakeholders about the importance of security and their responsibility. On one side, large enterprises wants to develop startup culture to boost innovation in the organization and attract new age young talent. Some of the groups in any organization always feel that they do very important and very different work and will push for security exceptions. Inconsistency in the policies is the biggest threat to an organization. Senior leadership need to explain their teams that exceptions create significant risk for the broader organization. On one side, when organizations need to build culture of trust, they also need to build culture of Trust but Verify. Organisations cannot just push for the culture of Trust sidelineing cyber security concerns else it will be like the silent bomb and companies may face large damage in the future. Cyber security culture need to be built across all layers of organisation including Board of Directors and senior leadership. It is not uncommon that senior leadership is worried about strategy to improve business performance, however ignorent about basic security measures on their smart devices like mobile antivirus or implementation of screen lock. For the sake of convenience, leadership often ask for exceptions for having the same computer or application password for years. Unless there is self awareness about cybersecurity in the leadership of the organisation, it is difficult to build it effectively across the organsiation. We also need to understand that cybersecurity is not the competitive advantage for any company. We need to spread awareness across the industry as breach of trust for any company may create doubts in the minds of customer across the entire industry segment or nation. It is everyones responsibility including Board of directors, leadership team, partner ecosystem, social communities to take active efforts in spreading cyber security awareness across the industries to make our

nation as most trustworthy and cyber resiliant nation.

CISOs: Leading from the front

It is one of the responsibilities of a Chief Information Security Officer (CISO) to implement the right policies and conduct risk assessments on an ongoing basis. CISOs must highlight the gaps to the board members and ensure their support in both reviewing the progress and investing in an upgrade of the security landscape. Companies should invest in cyber insurance to protect from risks that are beyond their control. Also, the role of CISOs has evolved into a challenging one, involving working closely with businesses, CIOs, CTOs and CDOs to understand their initiatives.

In last 2-3 years, the awareness, the need for and investments in cyber-security have substantially increased. With emerging new-age technologies and automation of security intelligence systems, cyber-security costs will go down significantly in the next ten years. According to a Cisco report, the world will have as many as 50 billion connected devices by 2020, which have to be secured as well. It will require a combination of the right technologies and skilled people to protect enterprises in the digital ecosystem.

Summary

To summerise, mounting a good defense requires understanding the offense. As we now understand, attackers have many options, such as DDoS assaults, malware infection, man-in-the-middle interception, and brute-force password guessing, to trying to gain unauthorized access to critical infrastructures and sensitive data. Measures to mitigate these threats vary, but security basics stay the same: Focus on prevention based technology. Keep your systems and security updates up to date, train your employees, configure your firewall to whitelist only the specific ports and hosts you need, Use next generation firewalls, End point detection and recovery solutions, Integrate seurity solutions for real time insights, get outside in view using cloud services for security analtyics, keep your passwords strong and use multi factor authentication, use a least-privilege model in your IT environment, make regular backups, and continuously audit your IT systems for suspicious activity.

Even if we build prevention based security architecture, we will not be able to protect organisation 100% from the new age threats. We also have to be proactive in detecting and responding effeciently with the attacks so that damage can be minimized. Organsiations need to invest in solutions for proactively monitoring confidential data leakage in the social media or dark web, credential leak monitoring, infrastrucutre and branding monitoring, vulnarabiity monitoring, monitoring BIN payment from the Dark web. In addition to monitoring IP, customer information and brand information leakage, companies must invest into cyber insurance to protect organisation from financial risk to certain extent.

To win the war against the cyber criminals, organizations need to understand the motivation behind cyber actions, advanced malware development, or macro industry trends. Once enterprise identifies the risk involved, they can think about the approach on how best to protect their businesses, including their people and critical data. Leadership team should ask Why is an end-user's communication not encrypted? Why is an attacker focusing their efforts on targeting a specific industry? Why did that obvious malicious behavior go undetected? Why employees are disclosing or storing confidential information on social media, personal email accounts or cloud based storages. We need to know that specific attacks will change and evolve, but the themes remain the same: sensitive data is an attractive target for attackers. Threat actors, malware authors, the "bad guys" will keep inventing new methods to bypass protection systems devised by the cybersecurity industry. Attackers and security analysts expend efforts in a continuous cycle of breach,

react, and circumvent, a true game of cat-and-mouse. We need to escape this game; by taking a step back every year to examine trends and motivations, relook at security architecture and redefine actions to build security culture.

9

Intricacies of Outsourcing and the Impact of Outsourcing on an Org's Security Landscape and Liabilities in an Outsourced Services scenario.

Mahindra & Mahindra - Hitesh Mulani, Group CISO & VP - IT Partner Collaboration & Process Excellence

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate

velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat c dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exerci-

tation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat c dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit inon proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat c

10

The Forgotten Story of "Insider Threat"

Wipro - Sridhar Govardhan, Chief Information Security Officer

An outsider or insider, who could be dangerous threat to an organization. In today's context the prominence and attention given to routine data breaches, malicious outsider gets highest priority when compared to a malicious insider threat. This phenomenon has created imbalance with respect to the attention required to protect organizations from insider threat.

By design, an organization trusts its's employee, temporary staff, contractors or business associates (insider) by enabling the required privilege and access to the organization's resources (internal practice, information, data and computer systems). Depending on the role and position of an insider in the organization, he/she would have distinct levels of access to the resources.

In a hypothetical situation, an individual or a group of colluding individuals who are entrusted with highest privilege go rogue against their employer. In such an event, the ramification could break the trust of the organization, monetary loss and plummeting impacting the brand value.

An insider is an individual, who could be employee, contract staff, vendor in an organization, who has end-to-end view of the process. The knowledge gained by the individual with respect to process, technology and people assist them in efficient performance of his / her role efficiently. The individual will have certain privileges in the ecosystem they are operating, which could be birthright assigned as part of the role or could be acquired privileges via approvals.

Financial institutions were early in the industry segment to embrace governance (as part of overall Risk governance) to manage insider threat, the model encompassed control implementation and monitoring of processes and technology usage by privileged roles. To mention a few,

- Segregation of Duties
- Multi-Level Approval
- Mandatory Job Rotation
- Enforcing Mandatory Vacation
- Internal & External Audits

The controls split the amount of power held by any one individual between two or more individuals or is validated by a peer. Few of these process controls where automated as part of automation and remaining were left as manual process.

Along with global economy, all sectors in industry grew, and to cater to the growing business demand and to handle the volumes of transactions, more and more business processes were automated and managed by select individuals. The controls deployed (automated and manual) remained static and couldn't scale with the growing demands. Over the years, due to high volume and manual control validation these controls lost its effectiveness thus leading to process and system flaw to insider attack.

A strong perception prevails about insider attack, encircling predominantly data theft and sabotage. Fraud by insider is least understood and is an underappreciated threat. Several recent frauds reported in India by banking sector and globally revels how these Insider's flew under the radar for years and went undetected from multiple eyes.

As per a survey conducted by Ponemon institute (https://www.observeit.com/cost-of-insider-threat/) , the average cost of insider threats per year for an organization is more than $8 million.

Further study of the reported cases, reveals many interesting realities about insider fraud and how they evade both deterrent & detection controls and deflect and checks and balances defined by the organizations. Upon close observation of each of these cases, we can categorize them into,

- **Orchestrated Fraud** – In this type of fraud, a single or group of individuals collude and hide a fraud from the system for multiple years.
- **Habitual Fraud** - An individual immaterial of job, role, location, he / she is posted, the pattern and modus operandi of the fraud remains same
- **Power of Collusion** – When multiple individuals come to gather and collude, they can evade multiple layers of controls, leading to colossal failure
- **Lone Wolf** – In lone wolf, a single individual will be involved in the fraud. Detection of lone committed frauds is the most difficult
- **Exploitation of known weakness** – Insiders are the individuals closest to the system, they are the people who use the system on regular basis and know all the weakness in the system and exploit to commit the fraud of humongous size
- **Timeline Fraud** – In this type of fraud, insider knows an exact time frame, during which the system will either have relaxed controls or is unmonitored. He / She uses this opportunity of time window to commit the fraud
- **Trusted Partner Involvement** – If a trusted partner, who is empaneled to evaluate the processes, gets involved and colludes with internal parties to commit fraud

By now it is evident, insider fraud is the hardest threat to detect and it takes long time to discover. The controls (automated & manual) designed and implemented to prevent and detect the insider fraud has failed to serve the purpose. The main reason for the failure is the controls implemented are "static" and inside perpetrators have understood the weaknesses of the controls.

Based on a fraud, an organization can perform a fine-tuning to strength the internal control, by adding additional checkpoints and human validations. This process will eventually crack after certain period and history will repeat.

Can this problem be solved permanently? Is there a silver bulled to insider fraud?

Whilst there is no silver bullet or permanent solution and silver bullet to this problem, we need to look at ways to complement the human element as much as possible when it comes to the decision

making and validation of the information. Artificial Intelligence (AI) enabled decision making and continuous surveillance, the platform should have the ability to integrate with other enterprise system.

The platform should use real-time information from external and internal sources and build intelligence about its users, process and operating environment. System should autonomously make decisions to approve or reject transactions based on multiple factors. If the AI system predicts a risk in the transaction the system should trigger decisive action to protect the process sanity and notify the anomaly.

The platform should independently work with ecosystem and,

- Brings the trustworthiness in the system
- Transform the process decision making with AI based automation, thus nullifying opportunities of an insider fraud
- End-to-End automated review and AI based workflow
- Provide continuous monitoring of health of the system
- Enables transparency of the transactions across the layers

Processes, which has dependency on human decisions or touchpoints are known to be defenseless to insider threats. Today enterprises have implemented touchless automation to ensure human involvement is minimal, the automated ruleset defined and implemented is static. The challenge with this is, insiders close to the process know the weaknesses of these static rules and this becomes weak points and could be exploited. AI based decision making safeguards each transaction using the perspective of multiple parameters. Implementers need to aware of AI's inherent weakness of "AI Bias", and ensure adequate safeguard is enforced.

Whilst this market segment is at its early stages with only few companies who are offering this kind of AI platform, which can integrate with the enterprise eco-system. Enterprises planning to adopt and operationalize these platforms should be prepared to customize their workflow and integrate with the platform for orchestration. With any security outcome, you will always need to look at how the technology and processes will work within ecosystem. There is no such thing as "set and forget" in security.

Contributor Profiles

Forbes Asia

JUSTIN DOEBELE

Executive Director – Content

Justin Doebele is one of the most experienced Forbes executives in Asia. He is currently the Executive Director - Content at Forbes Asia, based in Singapore from July 2018. Before that he managed and edited Forbes Indonesia from its launch in 2010. At Forbes Indonesia, he has led the team in creating one of the most successful business publications in the country, as well as launching ForbesLife Indonesia in 2014, now one of the most successful lifestyle media brands in the country. Before relocating to Jakarta, he was with Forbes in Singapore, where he set up the Singapore bureau for Forbes Global, and launched and managed the noted Asia Rich Lists for Forbes. He also played a major role in the launching of Forbes India, and worked closely with Forbes partners in China, Japan, Korea, Mongolia and Thailand. He has a BA from Harvard and MS in Journalism from Columbia University. He is the former president of the Jakarta Foreign Correspondents Club, the former Vice President of the Foreign Correspondents Association of Singapore, and a lifetime member of both the Singapore Press Club and the N.Y.-based Council on Foreign Relations.

Palo Alto Networks

SEAN DUCA

Vice President and Regional Chief Security Officer, Asia Pacific & Japan

Sean is vice president and regional chief security officer for Asia Pacific and Japan at Palo Alto Networks. In this role, Sean spearheads the development of thought leadership, threat intelligence and security best practices for the cybersecurity community and business executives.

With more than 20 years of experience in the IT security industry, he acts as a trusted advisor to organizations across the region and helping them improve their security postures and align security strategically with business initiatives.

Prior to joining Palo Alto Networks, he spent 15 years in a variety of roles at Intel Security, with his last position as the Chief Technology Officer for Asia Pacific. Before this, Sean was involved in software development, technical support and consulting services for a range of Internet security solutions.

Sean actively discusses security issues in mainstream media, including television, radio, print and security related broadcasts. He regularly participates in forums, conferences and panels, and provides intelligence on cybersecurity matters to the public and private sector.

Palo Alto Networks

ANIL BHASIN

Regional Vice President – India and SAARC

Anil Bhasin is the regional vice president for the India and SAARC region at Palo Alto Networks. Based in Mumbai, Anil leads the business and the Palo Alto Networks team in India.

Anil has over 25 years of experience in the industry, and joined Palo Alto Networks from Cisco, where he spent 12 years in leadership roles including the Services business for India & SAARC region.

Prior to joining Cisco, Anil had a two-year stint at Getronics (formerly known as Wang Global) in Dubai. As a National Sales Manager at Getronics, he was responsible for network integration for Cisco Systems. Anil was also a Senior Account Manager for M/s Computer World in Bahrain. During his six years tenure with M/s Computer World, he managed strategic accounts from the banking, government and manufacturing verticals, offering customized solutions and working very closely with principals such as Compaq, Acer, Microsoft, Novell Synoptics and Cisco.

Anil holds a diploma in computer engineering from Bombay Institute of Technology.

Capgemini

ERIC ANKLESARIA

Vice President & Global Leader- Banking & Capital Markets transformation

Eric is a Vice President and Global leader for the BCM transformation practice at Capgemini. Prior to joining Capgemini he worked as a partner leading the Financial Services IT Advisory practices of KPMG and Ernst & Young.

He is a skilled, results-oriented and performance-focused leader with over 17 years of experience (6 years as a Partner with 2 of the Big 4 global advisory and assurance companies). He comes with a broad-based management consulting experience in building and leading practices to deliver technology-centered initiatives across diversified financial institutions across banking, payments, asset management, and insurance industry sectors. Eric's broad experience encompasses large-scale core banking transformations, program management, IT strategy definition, CRM solution design and program management, packaged application selection and implementation, payments advisory, IT enabled business transformation, digital strategy and BI and analytics. He has worked extensively, both in the domestic and international markets like South Asia, Middle East, USA, UK and Eastern Europe, on some of the largest core IT and business transformation projects.

Eric has been nominated and has served as an active member of the Ministry of Finance committee on IT for the financial services sector. He has also had the privilege of chairing and placing the report to the Indian Banking Regulator (RBI) and the Ministry of Finance on the reforms needed in the Indian Payments and Settlement act and systems.

Cognizant

SARITHA AUTI

CSO, AVP Cyber security

A Cyber Security Practioner for 23 years, with in depth experience in Security product development and solution development for the Business Domains. She has extensively worked with Energy and Utilities, Manufacturing and Defence to devise Cyber Security solutions, threat intelligence platforms, Identity and Access Governance, Security Operations and Cloud Security solutions.

At present, Saritha heads the Cyber security Technology and Architecture for Cognizant Corporate, spearheading the IT and Cyber Security Transformation Programs. She has pioneered the Security Automations for SOC, Identity Lifecycle Management and building threat patterns. She is a believer of “Simplifying Security” both at Technology, Process and People level.

Data Security Council of India

RAMA VEDASHREE

CEO

Prior to moving to DSCI she was Vice President, NASSCOM leading all initiatives in Domestic IT, eGovernance and Smart Cities among others. At NASSCOM, she has also led the Healthcare initiative in partnership with apex Health Sector body, NATHEALTH and the NASSCOM-DSCI Cyber Security Task Force.

DSCI under her leadership is pursuing a Cyber Security Industry growth charter to make India into a global hub for cyber security and grow to 35B$ by 2025.

With a rich and varied experience of 28 years in the Industry, she has had long stints at NIIT Technologies, Microsoft and General Electric. Her previous roles include that of Director in Microsoft Global Services, and Vice President, GE India. She has experience in the diverse domains of IT consulting, Strategic Accounts and Business Development, e-Governance projects and Business Development for Infrastructure projects and Health and Water Sectors at GE.

She is member of many committees of Government of India, including the Data Protection Committee, Cloud Expert Group and Financial Inclusion Advisory Board.

A Gold Medalist from University of Hyderabad, she has also completed an Executive Education program from Harvard, and a short program in High Performance Computing from Cornell University.

Deloitte India

SHREE PARTHASARATHY

Partner, National Leader - Cyber Risk Services

Shree is a Partner and National Leader for cyber risk and security with more than 20 years of proven success in developing, managing and advising global enterprise clients on technology, security, risk management and compliance matters. At Deloitte, he is responsible for product development and innovation, service delivery, business development, client relationships, and P&L management.

He has experience in the strategy, design and implementation of solutions for enterprise technology and security infrastructure for cloud and non-cloud, social, identity management, disaster recovery, business continuity, fault tolerance, contingency and crisis management, application and infrastructure integrity, GRC, and managed services.

With proven success in performing risk assessments, technology and business audits, establishing global compliance programs, managing audits and compliance against regulatory/standards/leading practices, and establishing control environments, he has consulted and provided solutions in the areas of enterprise business and technology strategy, business process optimization and re-engineering, enterprise infrastructure design and optimization, establishing and managing global business and technology operations, and change management.

Shree has been invited as a speaker to various events across the world to share his thoughts in the field of Cyber Security. He has been invited by CII on various occasions as a key note speaker, and has also written several thought papers on Cyber Security and its various aspects.

GENPACT

RAMACHANDRA HEDGE

Vice President, Chief Information Security Officer

Ramachandra Hegde (Ram) serves as Vice President, Chief Information Security Officer for Genpact. Genpact is a global professional services firm focused on delivering digital transformation for its clients, guided by its experience running thousands of processes primarily for Global Fortune 500 companies. Genpact has 87,000 employees serving 800+ enterprises from25 countries. In his role as Genpact's CISO, Ram is responsible for enterprisewide information security, technology risk and compliance, digital product security and key technology and process aspects for data privacy.

Ram is passionate about information security, risk management and behavioral economics and the application of these disciplines to securely enable technological innovation and digital trust. Prior to Genpact, Ram served as Director, Global Information Security and Chief Information Security Officer for Praxair, Inc, a USD 13 Billion global manufacturer of industrial gases, in CT, USA. Prior to Praxair, Ram held increasingly responsible roles in information risk management with KPMG and PricewaterhouseCoopers.

Ram has over 23 years of experience in information risk management. He holds a Master of Science degree in Information Security and Assurance, with a concentration in Cybercrime and Critical Infrastructure, from Norwich University, USA. He holds the CISSP, CISA and CRISC certifications and is also a Chartered Accountant.

HDFC Bank

SAMEER RATOLIKAR,

Executive Vice President & Chief Information Security Officer

In his current role of Chief Information Security Officer & Executive Vice President at HDFC Bank, Sameer Ratolikar heads the Information Security Group and provides leadership to the development and implementation of Information & cyber Security program across the Bank.

A firm believer of CISO's role to be a business enabler, advisor and strategist , he has developed an information security vision and strategy that is aligned to organizational priorities and enables and facilitates the organization's business objectives, and ensure senior stakeholder buy-in and mandate

Prior he served as Chief Information Security Office with Axis Bank, where he was responsible for developing and implementing robust information strategies in line with business IT initiatives in a time-bound manner.

Sameer holds a bachelor of engineering degree in computers from Marathwada University.

IIIT Bangalore

PROFESSOR S. SADAGOPAN

Director

Professor S Sadagopan is the Director of IIIT Bangalore (since 1999); earlier he taught at IIM Bangalore (1995 - 99), IIT Kanpur (1979 -95) and also year-long / Semester-long teaching assignments at IIT Madras / AIT Bangkok respectively. He got his MS & PhD (1979) from Purdue University, USA and BE (Hon's) (1973) from Madras University. He has authored seven books, including "ERP A Managerial Perspective (Tata McGraw Hill) and dozens of scholarly papers.

He has travelled extensively across all the continents lecturing on all aspects of IT and written extensively for the Print Media (Times of India, Economic Times, Financial Express) since 1995.

He has served on the Boards of several PSU's (NMDC, Bank of India, Indian Overseas Bank, NLC Ltd., BEL, BEML), Private sector (Tata Elxsi, Informatics, Shawman Software) as well as NSE and NPCI. He has been on the Boards of several Universities including IIIT's in Bangalore, Dharwad, New Raipur, Delhi and Bhubaneshwar, VIT and Jain University.

He is an IT Adviser for several banks (Canara Bank, Union Bank of India, Syndicate Bank, Vijaya Bank, Bank of India, Indian Overseas Bank; PSU's (IOC, BPCL, BHEL, NTPC, BEL, BEML, NLC) and Private Sector Corporations (Ashok Leyland, Maruti, TTK). He served on the IT Sub-Committee of the RBI Board.

He has been involved with several major IT initiatives of the Government) that include Railway Reservation, Income Tax Computerisation, Khajane, SWAN, SDC, RTGS, MCA21 and AADHAAR. He has been on the Prime Minister's Task Force on IT / serving on Chief Minister's Task Force on IT for several States, including Karnataka, Jharkhand and Chhattisgarh

He is a Fellow of IEE (UK), Computer Society of India and Institution of Engineers.

He is a Fulbright Scholar

He was the recipient of several awards including "IT Pioneer Award" of Cisco (2015), Rotary Honour of Vocational Excellence (2010), Champion of Humanity, Hindustan Chamber of Commerce (2008)

KPIT Technologies

MANDAR MARULKAR

Chief Digital Officer

Mandar is Chief Digital officer at KPIT Technologies. In this role, he is responsible for creating digital offerings for customers, driving digital transformation for KPIT, building Think Digital culture, setting up Digital infrastructure and alliance ecosystem. In his earlier role, he was one of the top CIOs in India, Mandar is a much-decorated technology management professional. Acknowledged as a thought leader in numerous technology forums globally, Mandar has over 24 years of experience in diverse industries. He has demonstrated skills in effective execution of Digital and IT strategy and driving process innovation for enabling better insight in business operations providing transparency, predictability and enabling sustained growth. Mandar's expertise also extends in other areas like leading budget and resource optimization, post M&A integration/disintegration, planning risk mitigation and compliance measures..

Mandar started his tenure with KPIT 14 years back wherein he began with the management of IT systems. He has gone on to play various roles like Head Global Infrastructure, Chief Information Security Officer and Chief Information officer and now Chief Digital Officer. Last couple of years he has been leading the Digital Transformation at KPIT including implementing strategy for Digital Infrastructure, Infra as a code and cyber security. He has envisioned "Smart Enterprise" platform that leverages the digital technologies and has been instrumental in making our business "Smart".

Often introduced as a visionary CIO, Mandar has always been an early adopter of new trends and technologies. He backs the technology on its business value and focusses on how it can provide exponential business outcomes. Mandar serves on the customer advisory forums of leading OEMs and a technology speaker across various global forums. Mandar has featured in over fifty case studies and his interviews and articles have been published in various leading technology and business publications.

Mahindra & Mahindra

HITESH MULANI,

Group Chief Information Security Officer & Vice President - IT Partner Collaboration & Process Excellence

Wipro

SRIDHAR GOVARDHAN

Chief Information Security Officer

Sridhar is a recognized Cyber Security Leader, with accumulated over 18 years of professional experience. He is well known for leading organizational initiatives in building self-defensible enterprise network and promoting security conscious behaviour in employees. He has extensive experience in information security technologies, regulations and promoting security conscious behaviour in employees.

Sridhar has acquired 11 industry-recognized certifications in the domains of IT, Information Security, Security Framework and Secure Enterprise Architecture (SABSA, CISA, CISM). He holds a bachelor's degree in engineering and M. Tech from BITS Pilani; he has three patents in Cognitive Security.