Deloitte.

CII
Confederation of Indian Industry

Assessing Cyber Risk:

Critical questions for the board and the C-suite

November 2017

Foreword

"There are many ways of going forward, but only one way of standing still"

- Franklin D Roosevelt

Today's business corporations will already know that the government's attention has been on the board's duties in considering the interests of a broader group of stakeholders and aligning executive pay to corporate performance. The outcome that boards are invited to explain in annual reports about how they have taken account of broader stakeholders in their material decisions was likely.

You will be aware that cyber-crime is growing more rapidly than cyber security, and organizations have never been more at risk from cyber-attacks. Recent high-profile attacks on companies in the banking, health care, retail, and industrial sectors have highlighted the types of damage that can be done by hackers and cyber terrorists. This growing threat comes at a time when there is also an increase in focus from investors and regulators on how organizations manage risk. Company directors are informing themselves about the types of cyber threat their company faces, and the most important information assets and systems to monitor and protect. They are also better prepared to respond to a successful attack – and know who would be the company's spokesperson in case of a major data breach. It is not a question of whether there will be cyber-attacks-; it probably never was. It is a question of when, by whom and with what degree of expertise your company will be attacked.

While the digitally connected world of course presents threats, it also presents huge opportunities for those nimble enough to embrace them. The opportunity is not just about new business models, but also about the increased engagement with customers and suppliers, enabling better information exchange, increased efficiency and value accretion.

In this paper, we aim to give the board members a practical guide for enabling Cyber-Risk Intelligent governance. At the heart of the paper is a cyber-risk intelligent maturity model followed by 10 key questions representing "areas of focus," each of which signifies what we view as a key facet of cyber-risk governance. In each question, you'll find multiple criteria to gauge the cyber risk maturity of your respective organization. This is a set of questions that can help jump-start discussions among yourselves and with the management. The intent is not to imply a lack of reader attention, but to reflect and reinforce the importance of these themes across multiple aspects of achieving Cyber Risk Intelligent governance.

We hope you find this document useful in helping you guide your organization towards Risk Intelligence.

Deloitte

Contents

Assessing cyber risk: Critical questions for the board and the C-suite

Risk responsibility

Legendary basketball coach John Wooden once said, “Failure itself is not fatal, but failure to change might be.” Any company competing in today’s rapidly evolving business landscape should take Coach Wooden’s wisdom to heart. Effective cyber risk management starts with awareness at the board and the C-suite level. Sharpening one’s ability to understand risk, manage performance, and move one's organization closer to cyber maturity often begins with answering important questions. These answers should address issues pertaining to organizational security, vigilance, and resilience.

Prominent malware and attack methods continue to evolve, ingeniously bypassing prevailing security solutions. While 2016 witnessed sophisticated new malware emerging on a regular basis, exposing new capabilities, distribution methods, and attack services offered for sale through multiple platforms, 2017 is shedding light on a new trend – simple, yet highly effective malware families, causing greater and more rapid destruction globally.

A major, global cyber-attack could trigger an average of $53 billion of economic losses[1]

Most leading companies, their board of directors, and the C-suite have begun to address cyber security as a serious risk oversight issue that has strategic, cross-functional, legal, and financial implications. Consequently, necessary steps are being taken to enhance the cyber security awareness not just among employees but the management as well. India has made considerable progress in the last decade towards the establishment of Information and Communication Technology (ICT) infrastructure. India’s drive towards digital economy coupled with key national initiatives such as Digital India, Smart Cities, National Broadband Network are changing the digital landscape rapidly with direct impact on governance, transparency and accountability.

What does it mean to be secure, vigilant, and resilient?

Secure: Establish and continually maintain foundational security capabilities—by enhancing risk-prioritized controls to protect against known and emerging threats, while also complying with industry cyber standards and regulations.

Vigilant: Detect violations and anomalies through better situational awareness across the environment—within all areas of your ecosystem.

Resilient: Establish the ability to quickly return to normal operations and repair damage to the business following the inevitable cyberattack.

The following pages provide an in-depth look at 10 must answer questions which the leaders of all enterprises must consider to better comprehend where they stand when it comes to the “secure, vigilant, resilient” parameters.

1. Has your organization identified ownership to manage cyber security risk at the board and management level?
2. Have you built the right skills, experience and talent accountable for cyber security within the organization?
3. Have we established an appropriate cyber risk escalation framework that includes risk appetite and reporting thresholds?
4. Do the criteria to monitor and evaluate cybersecurity investments enable effective decision making?
5. Do the organization's cyber risk program and capabilities align to industry standards and peer organizations?
6. Are cyber-focused mindset and cyber-consciousness embedded in the organization culture?
7. Are efforts to protect the organization against third-party cyber risks adequate?
8. How efficient is the organization's cyber incident response program?
9. Do the criteria to evaluate the organization's cyber risk program enable efficient decision making?
10. Is your organization a strong link in this interconnected digital ecosystem?

Critical role of Boards and C-suite in helping their organizations respond to the constantly evolving cyber-threat landscape

Technology and Information are the cornerstones of digital transformation. Organizations can no longer evade the truth that Digital has become the need of the hour and the most effective enabler for creating a differential and unique competitive advantage. This transition to digital era has ushered in a new security paradigm and has brought to fore the challenges of cyber security.

Amid this evolving digital landscape, managing cyber-threats becomes a business and strategic imperative with the stakes higher than ever. Cyber risk has escalated so rapidly, and so publicly, that entities everywhere are scrambling to regain ground and keep pace with the evolving cyber threat.

Today, cyber risk and performance are more tightly intertwined. Tangible costs from cybercrime range from stolen funds and damaged systems to regulatory fines, legal damages, and financial compensation for the affected parties. Intangible costs could include loss of competitive advantage due to stolen intellectual property, loss of customer or business partner trust, and overall damage to the organization's reputation and brand.

Following are a few of the cyber security incidents that surfaced globally and in India in recent times:

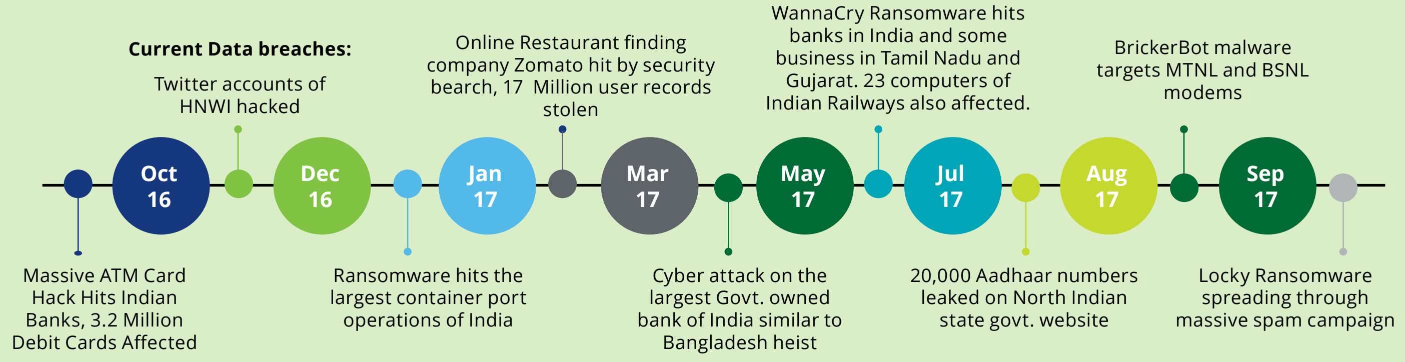
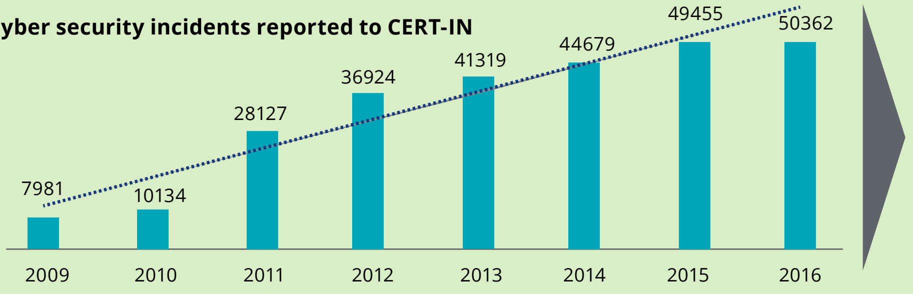

Current Data breaches:
Twitter accounts of HNWI hacked
Online Restaurant finding company Zomato hit by security bearch, 17 Million user records stolen
WannaCry Ransomware hits banks in India and some business in Tamil Nadu and Gujarat. 23 computers of Indian Railways also affected.
BrickerBot malware targets MTNL and BSNL modems
Oct 16
Dec 16
Jan 17
Mar 17
May 17
Jul 17
Aug 17
Sep 17
Massive ATM Card Hack Hits Indian Banks, 3.2 Million Debit Cards Affected
Ransomware hits the largest container port operations of India
Cyber attack on the largest Govt. owned bank of India similar to Bangladesh heist
20,000 Aadhaar numbers leaked on North Indian state govt. website
Locky Ransomware spreading through massive spam campaign

Figure 1: Cyber security incidents that surfaced globally and in India in recent times

Cyber security incidents reported to CERT-IN



129 Govt. websites hacked
8689 cases of fraud in ATM card

Incidents include phishing, scanning/ probing & denial of service attacks

10% of IT budget of Ministries to cyber security

The fast increasing number of breaches is leading to the need for strong cyber security policies and better security tools

India is witnessing an increase in targeted attacks including state sponsored attacks against Indian businesses and enterprises of all sizes in the last 5 years. As per the information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), security incidents have increased from 44,679 in 2014 to 50,362 in 2016. In the first half of 2017 (till June) 27,482 cyber security incidents were already reported.

Over 27,482 Cyber Security Incidents were reported in the first six months of this year to CERT-In.

Top-tier issue

With so much at stake, the board and the C-suite increasingly realize that it is time to fundamentally relook at how cyber security is positioned within the organizations. Cyber risk must be treated as a top-tier business risk and a boardroom issue requiring a deep level of awareness embedded in the culture of the organization.

Realizing that at some point the organization's cyber security will be breached, leaders should work to understand the most significant threats, and how those threats can put mission-critical assets at risk. There's no blanket solution to the challenge, but the board and C-suite leaders can begin developing a custom cybersecurity program or improve the existing one.

The 10 key areas that we lay out in the following pages should promote boardroom discussions around the management's ongoing cyber strategies: how leaders effectively address evolving challenges, how they mitigate cyber risks, and how they anticipate opportunities.

Assess your maturity level

This list of key cyber risk areas and accompanying range of responses should effectively guide organizations in assessing their cyber posture, challenge information security teams to ask the right questions and provide critical information, and help consistently monitor and improve cyber resilience going forward.

These questions are designed to help you identify specific strengths and weaknesses, as well as paths to improvement. Determine where your organization's responses to the following questions fall on the cyber maturity scale:

Initial/ Fragmented

Initiatives in the cyber risk management domain are negligible or next to non-existent wherein, mostly, the following are observed:

- Independent risk management activities
- Limited focus on the linkage between risks
- Limited alignment of risk to strategies
- Disparate monitoring and reporting functions

Integrated

Initiatives undertaken by the organization have a moderate impetus, are defined but partially operationalised wherein, mostly, the following are observed:

- Coordinated risk management activities across silos
- Risk appetite is fully defined
- Enterprise-wide risk monitoring, measuring, and reporting processes are defined
- Technology implementation is initiated
- Contingency plans and escalation procedures are defined
- Risk management training is planned
- Clear input into cyber security audit and other assurance activity plans

Cyber- Risk Intelligent

Multiple initiatives undertaken by the organization have a high impetus to cyber risk management program and such organizations are industry pioneers of efficient cyber security programs wherein, mostly, the following are observed:

- Risk discussion is embedded in strategic planning, capital allocation and product development
- Early warning risk indicators are used
- Linkage to performance measures and incentives is clearly defined
- Risk modeling/ scenarios are developed for efficient decision making
- Industry benchmarking is used regularly

1. Has your organization identified ownership to manage cyber security risk at the board and management level?

Determining the right degree of accountability at the leadership level is essential. In today's world of continually reported data breaches, boards cannot claim lack of awareness as a defence against allegations of oversight failures. Stakeholders and Regulators demand to showcase evidence of director attentiveness to cyber risk is only increasing.

Cyber Risk-intelligent

- Cyber Security is overseen by the full board
- At the management level, the Board has identified a C-level executive accountable for cyber security risk management including overseeing the enterprise's cyber security program decision-making, development as well as its implementation
- The board has one or more members who have expertise in Information Technology and cyber security and can interface with the board on a need basis. These members will be held accountable for the implementation of an enterprise wide cyber security risk management
- A concise high-level, 'simple English' cyber security strategic plan is agreed by the board and the senior management. Further, on a periodic basis the Board assesses these strategic requirements
- A dedicated senior management committee is established to oversee the enterprise wide cyber security program and to address any cyber security risks within the organization
- Monitoring the implementation of cyber security risk program through regular updates/dialogue between the board and the management. Also, the board is informed and updated about cyber risks and the potential impact on the organization

Integrated

- A concise and high level cyber security strategic plan is not defined
- The board has a high level oversight of the implemented enterprise wide cyber security risk management program and the cyber security risks/challenges occurring within the organization
- The board has working knowledge of Information Technology (IT) and cyber security risks
- Due diligence including monitoring of the cyber security risk program is lacking
- The board on an ad-hoc basis assesses the cyber security framework and strategic requirements

Fragmented

- The board and the management lack focus and understanding of cyber strategic issues
- Minimal involvement of the board and the senior management in cyber security related issues
- The enterprise lacks a governance mechanism such as an established Cyber Security framework. Further, Cyber security issues are left to those within Information Technology team/department to resolve with no board or management oversight
- Oversight of cyber risk and assessment of related budgetary requirements remains at a very high level

2. Have you built the right skills, experience and talent accountable for cyber security within the organization?

The major responsibility of the board is to ensure that the organization has the right talent to achieve its goals. It is important that the right skills and experiences are brought to bear in managing something as critical to the organization as cybersecurity. Everyone within an organization holds some responsibility for cyber risk. With many leaders busy performing their legacy duties, organizations may fail to identify and appoint an appropriate leader who will ultimately be accountable for cyber risk

Risk intelligent

- Board appoints a cyber leader at the C-suite level to align the organizational structure in line with the enterprise cyber security strategy and ensure the management has dedicated skills and experience to execute the strategy
- The cyber leader has a blend of both information security and business acumen to understand how the business operates to engage with the business, and prioritize risks and efforts
- The organization adopts a top down culture of accountability, collaboration and continuous education and training to manage cyber security risk. Cyber risk discussions take place at the board and the C-suite level
- Cyber security awareness amongst the management and the employees plays a key role. Employees stay up-to-date on the latest cyber trends, threats and implications for their business
- Every employee has an equally important role in protecting the enterprise from cyber security risks and intrusions. For this, the organization has appointed sufficient number of skilled staff with relevant industry experience
- Compensation and total reward programs are in-line with industry

Integrated

- Cyber leader is in place and primarily focused only on technical risks with minimal insight into business operations
- Cyber leader does not fully understand and appreciate how the organization operates
- Cyber risk has significant focus at Board and management level but the cyber risk discussions remain relatively at high-level

- Enterprise-wide cyber security awareness amongst the management and the employees is not optimal
- Skilled staff is present in IT and some business areas, but with limited industry-specific threat knowledge

Fragmented
- Minimal focus on cyber risk from the management and the leadership with no dedicated cyber leader identified
- IT function has taken up the role of cyber security and lacks complete understanding of business operations
- The organization does not adopt a top down culture to manage cyber security risks
- The management and the employees lack cyber security awareness
- Ad hoc training programs are developed for specific new technologies
- Significant employee attrition due to lack of investment in talent strategy

3. Have we established an appropriate cyber risk escalation framework that includes risk appetite and reporting thresholds?

As the cyber threat landscape evolves, managing cybersecurity risks is increasingly becoming complex. Relevant parties are seeking information and metrics on how effectively the organizations are addressing cyber security risks. It is imperative that organizations have a comprehensive and robust cyber risk framework in place and update the same on a continuous basis.

Risk intelligent
- Cyber Security framework is in place. This also includes a clearly defined Risk appetite statement approved by the board serves as foundation for the cyber security program and reporting
- The senior management has identified, prioritized, and reported the material or critical risks to the board through a risk prioritization process. Also, the senior management has provided detailed recommendations about the plan to the board, including identification of risks to be accepted, mitigated, or transferred (through cyber insurance)
- Risk appetite and cyber risks are identified and incorporated into the existing cyber security risk management program
- With evolving cyber security landscape, the established and approved enterprise-wide cyber security and risk policy is updated on an ongoing basis. Updated policy is also approved by the board
- Roles and responsibilities are clearly defined and documented in the Cyber Security policy. These roles and responsibilities are also implemented across the cyber risk program
- The board or the management committee reviews the annual risk self-assessment and evaluates the management's decisions to prioritize and allocate resources to address the results of the assessment
- Risk management review is included in the board's agenda with appropriate periodicity. As part of this review, those responsible for developing risk mitigation plans should address the risk profile of the company
- Key risk and performance indicators are defined, documented, and implemented. Processes and trigger mechanisms are in place to escalate threshold breaches to the senior management for significant or critical cyber incidents
- Reporting of cyber security incidents in line with Incident management framework includes escalation criteria aligned with the cyber risk program
- Mechanism to monitor and evaluate the value of the Cyber Insurance on an ongoing basis in place
- Monitoring and reporting of effectiveness of Cybersecurity investments on a periodic basis is in place

Integrated
- Cyber risk policy is defined but not consistently implemented across the organization. Implementation of the cyber security framework is limited only to certain departments
- Cyber risks are addressed only generally in the overall risk management and governance processes
- Risk prioritization and risk appetite are not integrated into the cyber risk framework
- Metrics and trigger thresholds are defined. However, the threshold breaches are escalated to the mid-level management and not to the management committee or to the board
- Risk management review is done by an alternate senior management committee on an ad-hoc basis and not by the board
- Cyber incident response is reactive rather than proactive
- No mechanism in place to evaluate the cyber Insurance value on an ongoing basis
- No mechanism in place to evaluate the effectiveness of cyber security investments

Fragmented
- Formalized cyber security framework is not defined and implemented to address cyber security risks within the organization
- Cyber Risk or incident escalation, if any, is on an ad-hoc basis and reactive
- Any cyber risk or cyber incident escalation is ad-hoc and does not adhere to any organizational governance policies and processes

4. Do the criteria to monitor and evaluate cybersecurity investments enable effective decision making?

With the trend of increasing cyber-crimes and reported data breaches, organizations across industry sectors are looking at increasing their cybersecurity spending to reduce, mitigate, and transfer their risks. Leaders should know what they're expending on resources including enhancing in house skills. Failing to develop a people strategy, overpaying for services, and other drags on operating costs are all very real risks

Risk intelligent
- Cyber security spend is aligned to the business objective as well as the cyber security strategy keeping in mind the industry trends
- The organisation has allocated security related budget which is aligned to the existing material risk (clear business cases for investments exist)
- Cyber security investments are focused on mitigation of material risks identified as a part of the risk review process and funds are strategically used to manage risks identified against business critical processes, functions and assets
- The organization tracks and evaluates the cyber security spends on an ongoing basis. Through reporting mechanisms based on metrics, the board and the senior management evaluates the effectiveness of implemented controls and in turn the cybersecurity spends

Integrated
- Cyber security spend is not completely aligned to the organization's strategy including industry trends
- Major cyber security investments are made in silos with no view of the of the organization's strategy
- Cyber security budget is bundled in other cost centers
- Difficulty in tracking the cyber security spends to justify expenditures
- Imbalance of security investment across baseline security controls and those required for highly sophisticated attacks

Fragmented
- Formal cyber strategy not in place
- Spend on cyber security initiative is ad-hoc with no investment plan in place
- Business case for cyber investment is rarely made
- The organization does not track the cyber security spends

5. Does the organization's cyber risk program and capabilities align to industry standards and peer organizations?

In today's connected and information heavy world, with so much at stake – organizational data, intellectual property and organizational reputation, cyber security has now become a boardroom issue rather than just an IT or technical administration issue. For this, the cyber leader should have a global view of the emerging business landscape and the cyber threats.

Risk intelligent
- The organization has a comprehensive and robust cyber security framework/program in place. This program is aligned to industry standards and the best practices to protect against and detect existing threats, remain informed of emerging threats, and enable timely response and recovery
- Leverage an industry framework as a baseline to manage the information security lifecycle
- An independent verification exercise is undertaken by the board to assess the status and effectiveness of the organization's cyber security program on a periodic basis
- On an ongoing basis, the organization reviews its internal compliance with the policies industry standards, and regulations. The review status is reported to the board and the senior management periodically for course corrections in the cyber strategy plan
- The organization has established baseline security controls at par with the industry. This may be achieved by obtaining ISO27001:2013 certification for its critical functions and applications

Integrated
- The organization has a cyber security framework in place but is not aligned to industry standards and leading practices
- Mechanism to review the effectiveness of the security program is conducted on an ad-hoc basis

- Updating the cyber security framework in line with the industry standards and leading practices is conducted on an ad-hoc basis
- Compliance to industry standards and other internal compliance program reviews may be undertaken occasionally but not consistently

Fragmented

- The organization does not have a formal cyber security framework in place and cyber security initiatives are implemented on an ad-hoc basis
- Compliance to industry standards and leading practices may be undertaken occasionally and on an ad-hoc basis
- May conduct intermittent high-level internal compliance reviews

6. Are cyber-focused mindset and cyber-consciousness embedded in the organization culture?

Cybersecurity, like all major risks, requires a culture of accountability, collaboration and continuous education and training, with all efforts geared towards supporting the strategy and mitigating cyber risks.

Risk intelligent

- 'Top Down' culture of cyber security exists within the organization
- The organization culture fosters individual cyber security awareness and acceptance of the strategy, and shared commitment to its implementation
- Executives are comfortable talking openly and honestly about cyber risk using a common vocabulary that promotes shared understanding
- The organization promotes enterprise wide cyber security awareness and education on an ongoing basis for all its stakeholders including the board, the management, the employees and the third parties
- Cyber security is viewed as a business enabler
- Cyber security awareness is ingrained in the operational tasks and activities and trainings are imparted to help the employees understand their cyber security responsibilities
- Employees understand that everyone has an equally important role to protect the enterprise from cyber intrusion and proactively seek to involve relevant parties on a need basis

Integrated

- Cyber security is not viewed as a boardroom issue and 'tone at top' indicates minimal C-level engagement in cyber security
- Understanding of cyber security risks across the organization is not consistent
- Focused training and awareness sessions on cyber security is not in place. Generic information security trainings are conducted
- Employees across the organization do not understand their cyber security responsibilities

Fragmented

- Cyber Security is viewed as deterrent by the management and the C-suite
- Cyber security is viewed as an IT administration issue
- Information Security policy including acceptable usage policy is defined and implemented
- The organization does not foster an understanding of cyber security and cyber risks
- Training and awareness sessions with regards to both generic information security and cyber security are conducted on an ad-hoc and 'need' basis

7. Are efforts to protect the organization against third-party cyber risks adequate?

In recent times, many breaches have their origins with the business partners, such as contractors and vendors. It is imperative in today's interconnected landscape that a business partner's cyber security controls are as robust as the organization's internal cyber security framework. The hackers, after all, target and exploit the weakest link in our digital ecosystem.

Risk intelligent

- Formal third party risk management framework is in place to engage third parties and contractors to outsource business processes
- The third party risk management framework is aligned to the organization's cyber security framework. It also takes into account the organization's risk appetite.

- As part of the vendor onboarding process, cyber risks are seen as part of the due diligence process and for the subcontracting arrangements
- Cyber security training, awareness and education is imparted to third parties and contractors on a periodic basis
- On an ongoing basis, as part of the third party risk management framework, all vendors and third parties must be profiled and assessed in line with the organization's expectations on the cyber security controls
- The organization's Incident management framework must establish formal processes for timely notification of cyber incidents stemming from third parties
- Steps are taken to mitigate potential cyber risks from outsourcing arrangements based on third-party profiling and risk assessments

Integrated

- Formal third party risk management framework is not aligned to the organization's cyber security framework
- Inconsistent processes are adopted for managing vendor lifecycle across the organization
- Due diligence around subcontracting and outsourcing activities is done on an ad-hoc basis
- Cyber security training, awareness and education is imparted to third parties and contractors on an ad-hoc basis
- Inconsistent review of risks as part of due diligence during the vendor lifecycle
- Steps are taken to mitigate potential cyber risks from outsourcing arrangements
- Vendors and third parties are profiled and assessed on an ad-hoc basis
- Incident notification by business partners and third parties is not contractually bound

Fragmented

- Formal third party risk management framework is not in place
- Third-party due diligence and cyber risk protection measures are not in place
- Third parties and business partners are not assessed to review the effectiveness of controls
- Cyber Security training, awareness and education is not imparted to third parties and contractors

8. How efficient is the organization's cyber incident response program?

Cybersecurity-related attacks have become not only more numerous and diverse, but also more damaging and disruptive. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring business operations.

Risk intelligent

- A formal incident management framework is in place in line with the organization's cyber security framework
- Cyber incident plans and procedures are developed for incident handling and reporting. Clear reporting and decision paths exist for incident handling and communication in response to a security failure or accident
- Cyber incident response policies and procedures are integrated with the existing business continuity management and disaster recovery plans
- Cyber incident response plans and procedures are rehearsed through simulations, and team interaction on a periodic basis
- Cyberattack exercise is conducted to review the effectiveness of the incident response plan on a periodic basis
- Relevant professionals/employees are made aware of their roles and responsibilities with regard to incident management activities
- External and internal communication plans exist to address cyber incidents for key stakeholders. These must be updated on a periodic basis
- For all employees, third parties and contractors awareness sessions, training and education with respect to incident management must be provided
- The organization is actively involved in industry simulations and training exercises

Integrated

- Formal incident management framework is not aligned to the organization's cyber security framework
- Basic cyber incident response policies and procedures are in place but not effectively integrated with the existing business continuity management and disaster recovery plans. Cyber incident response plans and procedures are rehearsed through simulations, and team interaction on an ad-hoc basis
- Cyberattack exercises are implemented intermittently across the business functions
- For all employees, third parties and contractors awareness sessions, training and education with respect to incident management are imparted intermittently
- Incident management policies, procedures and plans including communication plans are reviewed and updated on an ad-hoc basis

Fragmented

- Formal incident management framework is not in place
- Cyber incident response policies, procedures, plans and communication plans are not in place
- Simulations to rehearse cyber incident response plans and procedures are not conducted
- Awareness sessions and training with regard to incident management and incident response are not conducted

9. Do the criteria used to evaluate organization's cyber risk program enable efficient decision making?

Evaluation from end to end is the only approach in this area. While systems' expertise remains an essential ingredient of preparedness, it is only when cybersecurity is understood within the organization's overall risk management realm that executive leadership can have confidence that their single most important business asset — information — is sufficiently protected against today's threats, and tomorrow's.

Risk intelligent

- Formal reporting mechanism is put in place. Through this, the board and the C-suite can review the dashboards and reports published to assess the effectiveness of the cybersecurity program and appropriately manage the risks in line with the organization's risk appetite statement
- Periodic reviews, both internal and external, are conducted to assess the effectiveness of the implemented baseline controls
- The cyber security spend are tracked on an ongoing basis to ascertain the ROI on the implemented controls.
- The cyber security framework and the cyber risk program are updated on a periodic basis taking into account the evolving cyber threat landscape
- Lessons learned are applied to improve management of risk

Integrated

- Formal reporting framework/ mechanism is not in place. Reporting on the cyber security program to the board and the C-suite is done on an ad-hoc basis
- Basic cyber risk assessments are conducted on an ad-hoc basis
- Internal audit evaluates cyber risk management effectiveness not more than once a year
- Cyber security spend is not tracked and ROI on the implemented controls is not ascertained
- Lessons learned are sometimes, but inconsistently, applied to improve management of cyber risk

Fragmented

- Reporting to board or the C-suite is not in place
- Internal audit evaluations of the cyber security or the cyber risk framework are conducted on an ad-hoc basis
- Reactive approach is adopted to apply cyber security measures

10. Is your organization a strong or a weak link in this interconnected digital ecosystem?

With organizations undertaking digital transformation, interaction of various players of an enterprise i.e. customers, employees and business partners/third-parties through websites, social media, mobile devices, cloud, IoT and other advanced technologies is imperative and has increased the risk exposure. In this digital ecosystem, are you a weak link or a leader in cyber security? Collaborating with peer organizations and partners to share intelligence on threats is just one example of how business leaders can develop a more relevant, more holistic approach to cyber risk.

Risk intelligent

- Knowledge and information sharing with industry sector peers, independent analysis centers, the government and intelligence agencies, academic institutions, and research firms
- Networking within the organization is encouraged for sharing knowledge and information
- Strong relationships are maintained with all relevant stakeholders including external partners, law enforcement, regulators, etc.
- Participation in eminence activities such as industry forums to showcase and sharing of cyber security initiatives undertaken by the organization
- Independently enhance and maintain programs to avoid being the weakest link

Integrated

- Knowledge sharing with industry peers and government agencies done on an ad-hoc basis
- Networking within the organization for sharing knowledge and information is not in place

Fragmented

- Relationships are not maintained with all relevant stakeholders including external partners, law enforcement, regulators, etc.
- No knowledge and information sharing with industry sector peers, independent analysis centers, government and intelligence agencies, academic institutions, or research firms

In addition to the above questions, it is time to evaluate digital risk readiness by asking questions based on these dimensions:

- Digital Footprint: Do you know what digital activity you own and how others use your brand online?
- Digitally Aligned?: Is your digital activity aligned with your business objectives?
- Operations: Have you set the rules of engagement with digital through appropriate policies and procedures?
- Assurance: Do you regularly monitor the performance and compliance aspects of your digital footprint?

A strategic approach towards goal setting

Setting a target state for cyber resilience is vital at any level of maturity. Cognizance of the risks that your enterprise may counter may not feed the organizational immunity well. It is also crucial to understand the business context and priorities.

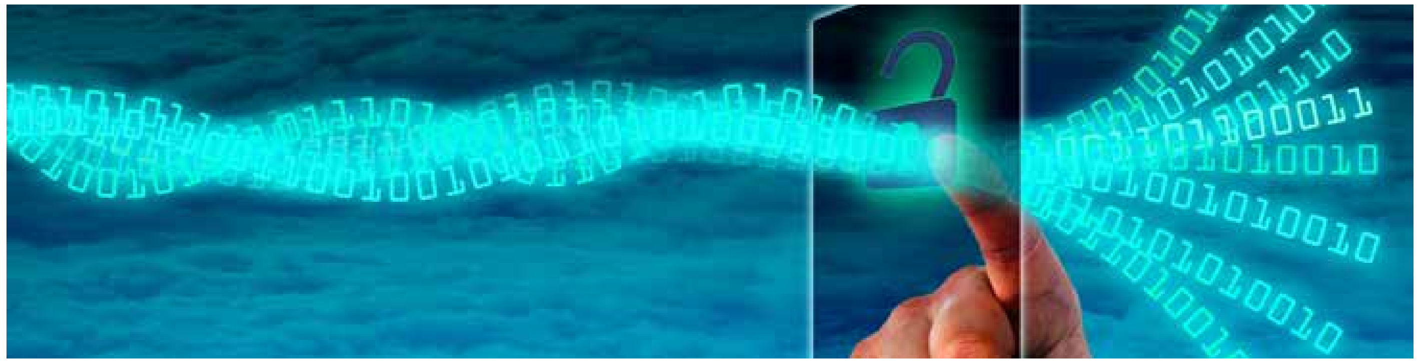
It is not expected or required that all organizations achieve the highest level of cyber maturity. The type of business, its scope, and vision greatly determine the optimum level of maturity for an enterprise. Clearly, a one-size-fit-all approach is not something that will work while setting the target state for cyber resilience and maturity. Besides, the time and cost involved in achieving the desired state should complement the business strategy and setting. The idea is to build a cyber-risk vigilant culture and attitude that engenders an ongoing endeavor towards evolution in risk practices in areas that are deemed critical. And this idea extends beyond just spending money for an advanced, mature cyber resilience infrastructure; it encompasses adopting optimized methods that help you invest in programs that identify your organization's specific needs and provide corresponding "tailor-made" solutions that continuously drive your organization towards being holistically secure, vigilant and risk-intelligent.

Where do you stand?

Based on the results of your assessment, does your current state of maturity support or hinder your strategy and mission? If your maturity index is not aligned with your target state of maturity—or if you have not yet developed appropriate cyber goals—it's time to start enhancing your cyber risk posture.

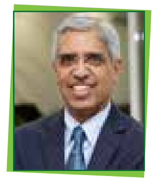
Of course, it isn't possible for any organization to be 100% secure, but it's entirely possible to manage and significantly mitigate the impacts of cyber-threats, including theft, regulatory penalties, legal compensation, and reputational damage. Over the past eight years, the only constant has been change. We hope the above assessment enables your organization to develop the dexterity and vision required not only to overcome operational inertia but to thrive in a business environment that is, and will remain, in flux.

While this is no small task. Though the technology advances we see today embody potential, only a select few may ultimately deliver real value. Indeed, some are more hype than substance. We need to do a better job of sifting through the noise to identify truly ground breaking innovations that can deliver value. Then, we need to act. Passively wondering and waiting are not the options. As explained in Newtonian physics, the task before us is turning energy's potential into reality!



Contact

Rohit Mahajan
President – Risk Advisory
Deloitte Touche Tohmatsu India LLP
rmahajan@deloitte.com



A.K.Viswanathan
Partner – Risk Advisory
Deloitte Touche Tohmatsu India LLP
akviswanathan@deloitte.com

Abhay Gupte
Partner – Risk Advisory
Deloitte Touche Tohmatsu India LLP
agupte@deloitte.com

Shree Parthasarathy
Partner – Risk Advisory
Deloitte Touche Tohmatsu India LLP
sparthasarathy@deloitte.com

Munjal Kamdar
Partner- Risk Advisory
Deloitte Touche Tohmatsu India LLP
mkamdar@deloitte.com

End Notes:

Deloitte University Press, Tech Trends 2017. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology/gx-tech-trends-the-kinetic-enterprise.pdf

Deloitte whitepaper on 'Evolution in the Indian Cyber Security Landscape', 2017

AICPA press releases, http://www.aicpa.org/Press/PressReleases/2016/Pages/AICPA-Proposes-Criteria-for-Cybersecurity-Risk-Management.aspx

[1]Reuters, https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB

https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF

http://www.sebi.gov.in/legal/circulars/jul-2015/cyber-security-and-cyber-resilience-framework-of-stock-exchanges-clearing-corporation-and-depositories_30221.html

https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo3118&flag=1

http://www.sebi.gov.in/legal/circulars/sep-2017/cyber-security-and-cyber-resilience-framework-for-registrars-to-an-issue-share-transfer-agents_35890.html

http://www.trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf

CII

Confederation of Indian Industry

The Confederation of Indian Industry (CII) works to create and sustain an environment conducive to the development of India, partnering industry, Government, and civil society, through advisory and consultative processes.

CII is a non-government, not-for-profit, industry-led and industry-managed organization, playing a proactive role in India's development process. Founded in 1895, India's premier business association has over 8,500 members, from the private as well as public sectors, including SMEs and MNCs, and an indirect membership of over 200,000 enterprises from around 250 national and regional sectoral industry bodies.

CII charts change by working closely with Government on policy issues, interfacing with thought leaders, and enhancing efficiency, competitiveness and business opportunities for industry through a range of specialized services and strategic global linkages. It also provides a platform for consensus-building and networking on key issues.

Extending its agenda beyond business, CII assists industry to identify and execute corporate citizenship programmes. Partnerships with civil society organizations carry forward corporate initiatives for integrated and inclusive development across diverse domains including affirmative action, healthcare, education, livelihood, diversity management, skill development, empowerment of women, and water, to name a few.

The CII theme for 2017-18, **India Together: Inclusive. Ahead. Responsible** emphasizes Industry's role in partnering Government to accelerate India's growth and development. The focus will be on key enablers such as job creation; skill development and training; affirmative action; women parity; new models of development; sustainability; corporate social responsibility, governance and transparency.

With 67 offices, including 9 Centres of Excellence, in India, and 11 overseas offices in Australia, Bahrain, China, Egypt, France, Germany, Iran, Singapore, South Africa, UK, and USA, as well as institutional partnerships with 344 counterpart organizations in 129 countries, CII serves as a reference point for Indian industry and the international business community.

Confederation of Indian Industry
The Mantosh Sondhi Centre
23, Institutional Area, Lodi Road, New Delhi – 110 003 (India)
T: 91 11 45771000 / 24629994-7 • F: 91 11 24626149
E: info@cii.in • W: www.cii.in

Follow us on:

facebook.com/followcii   twitter.com/followcii   mycii.in www.mycii.in

Reach us via our Membership Helpline: 00-91-124-4592966 / 00-91-99104 46244
CII Helpline Toll free No: 1800-103-1244

CII

Confederation of Indian Industry

Without limiting the rights under the copyright reserved, this publication or any part of it may not be translated, reproduced, stored, transmitted in any form (electronic, mechanical, photocopying, audio recording or otherwise) or circulated in any binding or cover other than the cover in which it is currently published, without the prior written permission of CII and Deloitte. All information, ideas, views, opinions, estimates, advice, suggestions, recommendations (hereinafter 'content') in this publication should not be understood as professional advice in any manner or interpreted as policies, objectives, opinions or suggestions of CII or Deloitte. Readers are advised to use their discretion and seek professional advice before taking any action or decision, based on the contents of this publication. The content in this publication has been obtained or derived from sources believed by CII and Deloitte to be reliable but CII and Deloitte do not represent this information to be accurate or complete. CII and Deloitte do not assume any responsibility and disclaim any liability for any loss, damages, caused due to any reason whatsoever, towards any person (natural or legal) who uses this publication. This publication cannot be sold for consideration, within or outside India, without express written permission of CII and Deloitte. Violation of this condition of sale will lead to criminal and civil prosecution.

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.