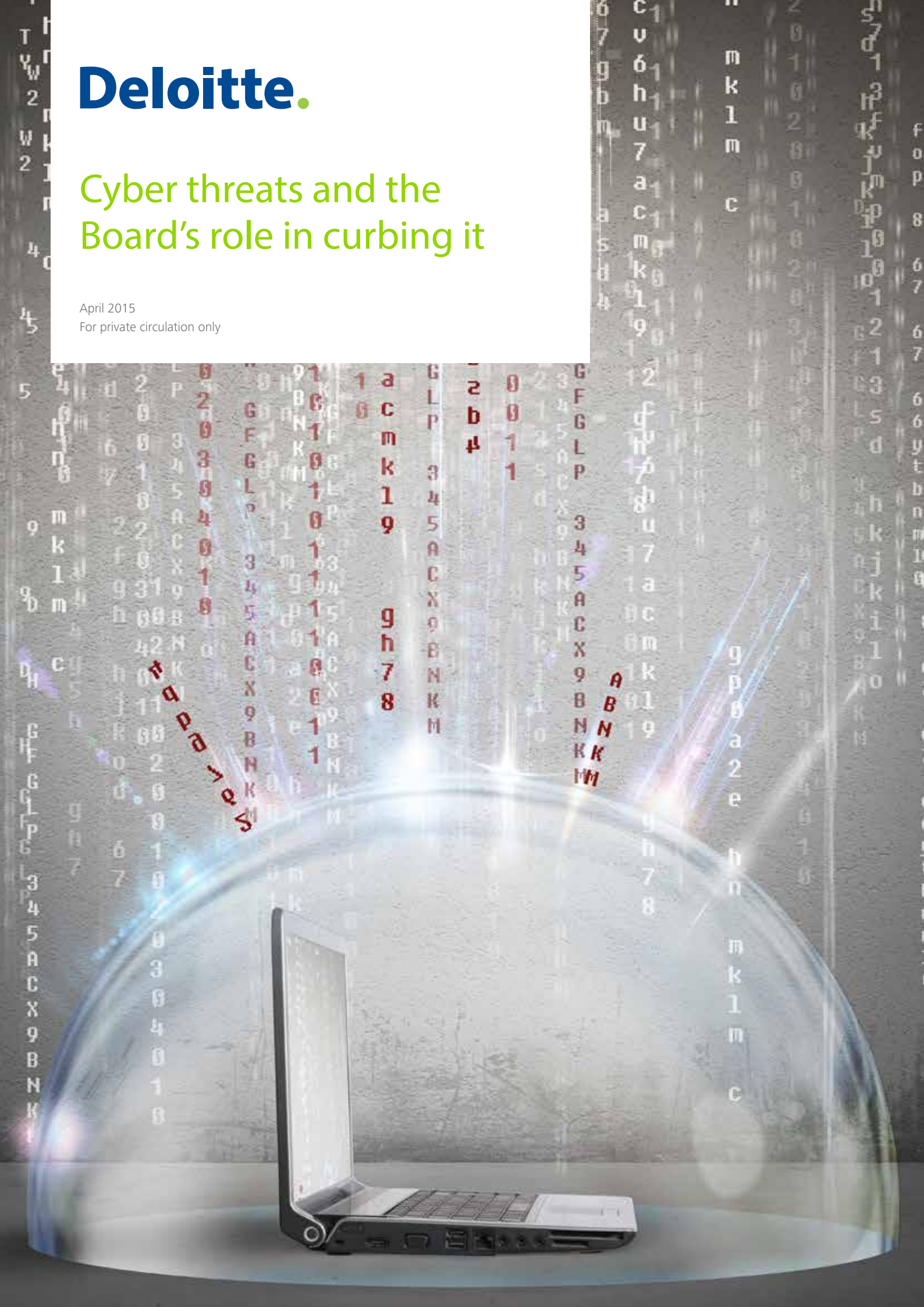
Deloitte.

Cyber threats and the Board's role in curbing it

April 2015
For private circulation only



Cyber threats and the Board's role in curbing it
A point of view

Technology is impacting businesses like never before. While, traditional businesses are adopting e-platforms to widen their reach, new businesses based solely on new technologies like social, mobile, analytics and cloud (SMAC) are growing at breakneck speed. The Internet of Things (IoT)[1], where interconnected devices could monitor various aspects of professional and personal life using internet-based technology, is fast becoming a reality.

Although smart devices connected to the internet will make lives simpler, they are also likely to expose individuals and organizations to cyber threats.

We are seeing a rapid increase in the prevalence and sophistication of cyber-crime and cyber espionage compromising organizational networks and data. These incidents increase an organization's risk of fraud, intellectual property theft, network incapacitation and damage to brand and corporate reputation – all of which can have far reaching and expensive consequences. It would be therefore prudent, if organizations can spend more time understanding these cyber threats and developing specific measures to address them.

[1]The Internet of Things refers to the interconnection of uniquely identifiable computing devices using existing internet infrastructure. Examples of IoT include thermostats/ washing machines that use WiFi for their operation and remote monitoring, and wearable devices like pedometers that connect to applications on your phone to give real time statistics and monitoring provisions.

Understanding cyber threats and its motivations

Unlike other fraud, the motivations for perpetrators of cyber threats extend beyond financial gain and include revenge, personal thrill, activist causes, deep rooted anti-establishment sentiments, and a need to prove self-worth by showcasing professional finesse in hacking complex security systems. The perpetrators of cyber-attacks can, therefore, range from individuals or small groups of insiders, suppliers and activists, to large-scale organized efforts by criminal networks and foreign entities.

Hence, cyber-attacks can vary in nature and include scenarios - such as introduction of malicious software like trojans, worms, viruses and spyware; password phishing; and denial-of-service attacks intended to crash websites. Each type of attack presents unique challenges and requires a targeted set of prevention activities, not all of which may be related to technology controls. Phishing or social engineering techniques, for instance, are often dependent on employees divulging their password or other sensitive information when requested under false pretense. Thus, education and awareness across the organization of policies and the reasons behind them are of paramount importance in preventing losses.

In our experience, corporate India has a limited understanding of the above mentioned risks. While data disclosures (authorized or otherwise) was recognized as the most significant cyber fraud risk concerning organizations in the Deloitte India Fraud Survey conducted in 2014, only 14 percent of survey respondents indicated awareness of data loss or leakages arising from hacking or hijacking of cloud based services. Further, over 61 percent of the survey respondents indicated the absence of a formal policy or training/ sensitization program for employees on using social media in their organization.

Organizations intending to address cyber fraud need to start by recognizing that cyber frauds require a dedicated fraud risk management policy and a team that can proactively manage these fraud risks. This is where the Board of Directors can play a significant role.

Managing cyber threats – Role of the Board

As recent as five years ago, it was rare for the Board of Directors to be closely involved in managing cyber security risks. But the growing magnitude of cyber fraud and the corresponding potential losses (of reputation and customer trust) are forcing the board and audit committee to devote increased attention and resources to respond to cyber threats.

To improve their preparedness to tackle cyber threats, Board of Directors can focus on the following leading practices:

1. Become aware of cyber threats - Whether or not there is a dedicated risk committee on the Board, it is important to have directors with knowledge and skills pertaining to security, IT governance and cyber fraud. Periodic training/ workshops can be organized for directors to come up to speed with the developments in the world of cyber fraud.

2. Coordinate cyber threat initiatives - In its capacity of overseeing risk management activities and monitoring the management's policies and procedures, the Board plays a strategic role in coordinating cyber threat initiatives and policies, and confirming their efficacy. These responsibilities include setting expectations and accountability for the management, as well as assessing the adequacy of resources, funding and focus for cyber security activities. The Board can leverage the audit committee chair as an effective liaison with other groups, in enforcing and communicating expectations on security and fraud risk mitigation.

3. Appoint a senior management person to develop a cyber- threat response plan – It is recommended that the Board appoint a Chief Information Officer, focused on information security, so that there is a clear voice directing cyber threat prevention, remediation and recovery plans, related educational activities, and the development of frameworks for effective reporting.

4. Leverage external specialists to review cyber threat response plans - External specialists can often be a valuable source of information on cyber security issues for evaluating and strengthening security controls and implementing programs for cyber fraud risk management. Specialists can also provide recommendations on key performance indicators that can be used to evaluate and monitor cyber threats.

5. Seek independent external specialists to assess cyber security measures – Boards can prompt companies to seek independent specialists to conduct annual reviews of security and privacy programs, including incident response, breach notification, disaster recovery and crisis communication plans. Such efforts can be commissioned and reviewed by the board's risk committee or another designated committee to confirm that identified gaps or weaknesses are addressed. Third-party security assessments can also provide benchmarking relative to other companies of similar size or in the same industry.

6. Availability of experts to respond to incidents of cybercrime – Electronic evidence is delicate and can be easily altered, damaged or destroyed with improper handling or delay in response. Having a team of in-house specialists or recruiting a third party expert organization with access to technology labs can ensure that evidence is collected carefully and response to such incidents is timely.

While implementing some of the above measures, Boards need to understand that cyber threats continue to evolve, and therefore response and fortification against cyber threats also needs to be an evolving process.

Checklist to establish better cyber threat risk governance

In our experience, the measures listed below can provide the Board of Directors with a high-level guide for establishing a cyber- threat risk governance program.

Stay informed about cyber threats and their potential impact on your organization.

Recognize that cyber threat risk intelligence is as valuable as market intelligence.

Assign senior management accountability for cyber threat risk management. This includes monitoring of current and proposed legislations and regulations in this area.

Provide sufficient resources for the organization's cyber threat risk management efforts, including third party experts.

Empower the management to conduct regular, substantive reports on the organization's top cyber threat risk management priorities.

Arm executives with tools to track and report metrics that quantify the business impact of cyber threat risk management efforts.

Enable executives to establish continuous monitoring methods that can help the organization predict and prevent cyber threat related issues.

Ensure that the internal audit team evaluates cyber threat risk management effectiveness, as part of its quarterly reviews. Recognize that effective cyber threat risk management can give your organization more confidence to take calculated risks (e.g. adopting cloud computing) to pursue new business value.

[2]This high level guide is not a substitute for formal, rigorous IT security assessments performed by specialists.

Looking Ahead

Cyber security is becoming a key concern for most Boards, and Directors should consider becoming more proactive in evaluating cyber threat risk exposure as a fraud risk management issue and not limit it to be an IT concern. To assess their current preparedness to manage cyber threats, Boards can ask the following questions:

- Is there a Board member who serves as an IT expert and understands cyber risks?
- Does the organization have cyber insurance?
- Is there a committee assigned to address cyber security?
- Does the organization have a chief security officer who reports outside of the IT organization?
- Is social media a concern for the organization?
- Do outsourced service providers and contractors have controls and policies in place to handle sensitive information and do they align with our organization's expectations?
- Is there an annual company-wide education/ awareness campaign focused on cyber security?

If the answer to any of these questions is 'No', it is time for the Board to step in and take charge.

Contacts

Rohit Mahajan
Senior Director and Head
Forensic
Tel: +91 22 6185 5180
Email: rmahajan@deloitte.com

Veena Sharma
Director
Forensic
Tel: +91 22 6185 5213
Email: vesharma@deloitte.com