Cyber Mastery Matrix

Securing your enterprise against the next attack

2020

CONTENTS

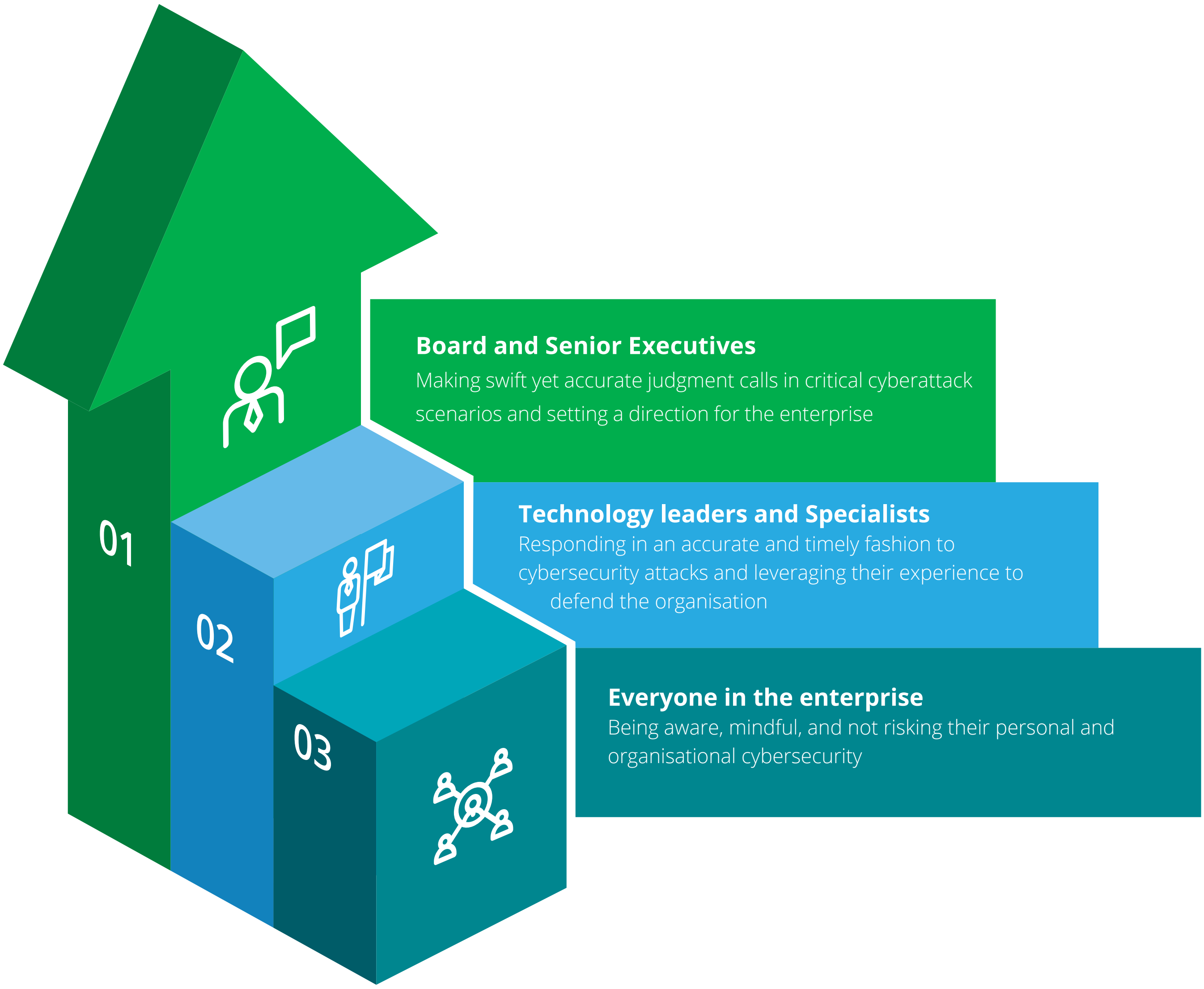
Are you prepared to face the unknown?

With threat actors striking as frequently as every 39 seconds[1] any enterprise could be a potential target for a cyberattack. The question is never if, but when, the next cyberattack will be. If your enterprise is resilient, you can recover swiftly and with minimal damage when cyber criminals come knocking.

The first step towards tackling unknown risks and improving your organisation's security posture, is to identify security gaps that can be leveraged by threat actors. Analyses of cyberattack cases have revealed that it's not only technology breaches that have led to security incidents, but also the actions of well-meaning employees and their preparedness levels during a cyberattack, which can be exploited by cyber criminals.

It is crucial to understand the various roles employees and C-suite executives play in enabling a secure enterprise. By taking into account the unique challenges they face, employees can be empowered to play a definite role in reducing cyber risk.

At Deloitte India's Risk Advisory, we believe that cyber is not just technology-focused, but has the power to influence key business decisions through the right awareness channels and actions of:



Board and Senior Executives
Making swift yet accurate judgment calls in critical cyberattack scenarios and setting a direction for the enterprise

Technology leaders and Specialists
Responding in an accurate and timely fashion to cybersecurity attacks and leveraging their experience to defend the organisation

Everyone in the enterprise
Being aware, mindful, and not risking their personal and organisational cybersecurity

Your first step to tackle the unknown – acknowledge the challenge in front of you

The threat landscape is continuously evolving. To gauge if your workforce is prepared to protect, defend and respond to cyber adversaries, you may consider evaluating key statistics. These statistics give rise to questions regarding business challenges that an enterprise is faced with, and are especially crucial for the CIO/CISO executives. The real differentiating factor is building an approach to cyber-readiness by answering the questions below:

$133.8 billion	Worldwide spending on cybersecurity is forecast to reach $133.8 billion in 2022[2]	What investments can I make in my employees to ensure they are equipped to face industry-specific challenges and stay one step ahead in a dynamic cyber landscape?
82 percent	82 percent of employers report a shortage of cybersecurity skills[3]	Are employees at every level of my enterprise equipped, informed and skilled to handle zero day panics and be resilient in the face of an attack?
32 percent	32 percent of 500 C-suite executives defined the most concerning cyber threat as actions of well-meaning employees. This is among the top three concerns, and superceeds technical vulnerabilities which stand at 31 percent[4]	As cyber risk becomes a board room discussion, is there a solution that prepares my workforce for targeted attacks and expedites the transformation of its cost and efficiency parameters?
206 days	The average time elapsed before detecting a data breach is 206 days, and the mean time to contain a breach is 72 days[5]	How do I ensure my enterprise is supporting the leadership in detection and containment of a breach?

A large-sized enterprise in India incurs an average economic loss of US $10.3 million from cyberattacks, whereas a mid-sized enterprise incurs an average loss of US $11,000[6].

Apart from financial losses, cyberattacks can also have multiple consequences that could stall overall growth in the short-term and impact business sustainability in the long run. A few such scenarios include:

- Exposure of sensitive data such as stolen credentials that can be leveraged against the enterprise and its employees
- Attacks on critical infrastructure that can lead to loss of life
- Disruption in efficiency that can impact your overall IT operational expenditures
- Denial of service attacks that can stall your business operations
- Compromised brand reputation that can lead to loss of your customer's trust

Enterprises must invest in upskilling and increasing cyber awareness to improve the preparedness quotient of their employees. This, in turn, not only reduces human errors, but also significantly improves incident detection and response. The solution to achieving a cyber secure future lies in adopting a structured, end-to-end approach to security.

Enter the matrix for futuristic solutions to your impending trials

Our Cyber Mastery Matrix service is a suite of tailored solutions that empower you to conquer all the dimensions of cybersecurity, leading to a secure future. It seamlessly embeds cyber in the DNA of your enterprise's strategy, and gives it the prioritisation and focus it deserves. By catering to the varying cybersecurity needs of different employee groups in your enterprise, it fosters a sustainable security culture that increases your cyber maturity as a whole.

Today's evolving business and operating environment with increased convergence and mobility furthermore requires every employee and leader in the enterprise to play a meaningful role. The Cyber Mastery Matrix will empower your employees to propel your enterprise forward in an era of digital transformation.

CYBER WARGAME

All cyber crises are unique and require preparedness and prompt decisions by executives for their containment. Tackling an attack may include negotiations with hackers, implementation of cyber response tactics, trade-offs between uptime and security, and selection of optimum recovery options considering the damage to the enterprise and its reputation.

Industry-aligned and customised cyber wargames are an important way to educate employees in preparedness and strategy to handle a complex cyber crisis. They also aid an in-depth understanding of cyber risk management and the adaptive response capabilities the enterprise will require during, after, and while preparing for the next cyber crisis. While traditional assessments evaluate security controls and processes, cyber simulations provide top executives with the immersive experience of responding to a cyberattack.

With our experience of conducting and delivering numerous wargames, we help evaluate your current preparedness and further strengthen the resilience of your enterprise. The Cyber Wargame solution is built to emulate a real-world cyber crisis in a secure and controlled environment. It is specially designed for board members and C-Suite management executives, and is delivered by Deloitte industry leaders and top cyber experts. It offers tailor-made simulations unique to your enterprise, backed by Deloitte's global experience and expertise. It customises response strategies for your enterprise to enable you to stay ahead of the curve.

Cyber Wargames enable a holistic understanding of threats and their impact, resulting in faster decision-making with respect to policies and building business resilience.

Cyber Wargame experience by Punit Renjen, CEO, Deloitte Global

"Recently, I joined two dozen Deloitte Global leaders for a four-hour wargame exercise to test Deloitte's ability to assess and respond to a simulated global cyber breach. The wargame was led by two Deloitte Risk Advisory leaders, who run these events for clients around the world. Our group was put through the paces as we dealt with disruption to operations, data exfiltration, media coverage, and client and regulator requests for information. While the event was only a simulation, let me assure you, the adrenaline we felt was real.

The fact is, cyber threats are the new normal. We cannot assume we are immune to hackers and cyber thieves. But, we can be prepared to respond swiftly and appropriately to a cyber-event and, we can take ownership for the role each of us play every day in keeping our enterprise safe."

Here is how Cyber Wargames reduce operational costs and lower the time essential for the growth of your enterprise

Leadership and board members

Duration

4-8 hour long interactive, simulation -based exercise

Description

- Simulates industry and function specific incidents for your top management and board members to participate in, to enable executive decision-making
- Evaluates the crisis preparedness of your enterprise for various cyber threats, and in turn the current resilience strategy

Technology and risk leaders; CISO, CIO, CTO, CRO

Duration

1-2 day long scenario-based, war game exercises

Description

- Creates complex real- world scenarios to empower leaders to reduce the lifecycle of an incident, from breach to containment
- Evaluates the design of the cyber incident response plan of the enterprise by simulating an enterprise grade IT and systems network
- Serves as a playground for increasing synergies between the key technology functions

CYBER TRANSCEND – SIMULATION AND RANGE

With the introduction and advent of digital technologies, there are now multiple layers within an enterprise's infrastructure. These result in greater complexity, as well as expose its systems to newer vulnerabilities. Protecting the enterprise and making it resilient in the shortest possible time will be the key focus of any CXO to ensure business continuity. Upskilling the IT and cybersecurity teams, equipping them with the right tools, and focussing on hands-on experience of real-world scenarios is the need of the hour.

Our Cyber Transcend solution enables you to train on real set-ups and learn sophisticated cyberattack patterns and defense techniques from professionals. It allows you to:

- Discover and innovate cyber resilience strategies with the help of cutting-edge content and methodology
- Immerse yourself in a sophisticated environment that simulates real cyber incidents under expert guidance to take you through defensive and offensive techniques
- Build a confident team within a short time frame through practical trainings, using cyber defense tools and real-world attack mechanisms

Cyber Transcend offers a range of solutions using the simulation platform in our Cyber Experiential Center that will equip your security professionals to stay one step ahead of the attacker.

IT and cybersecurity teams (Professional)

- Enterprise incident handling and response
- Advanced intrusion detection and defensive techniques - An intriguing Blue Team essential
- Advanced offensive techniques and hands-on hack labs - Red Teaming mastery
- Capture The Flag (CTF) events
- Cybersecurity fluency for professionals
- Malware analysis
- ICS/SCADA security simulation

Mid-level and Senior Management (Advanced)

- Cyber fluency for executives
- Enterprise incident handling and response
- Malware analysis
- ICS/SCADA security simulation

Employees across all functions (Basic)

- Enterprise incident handling and response
- Malware analysis
- ICS/SCADA security simulation

CYBER ACADEMY

Embedding security awareness in the DNA of each employee develops in them a strong sense of personal responsibility and accountability. A sustainable and transparent security culture in an enterprise can be fostered by empowering security behaviour, which will eventually increase the overall cyber maturity of the enterprise.

Cyber Academy is a customisable, participative and measureable solution that understands the current level of awareness of an enterprise, defines a strategy, and develops a recognisable awareness campaign for all employees from a graduate hire to the top management.

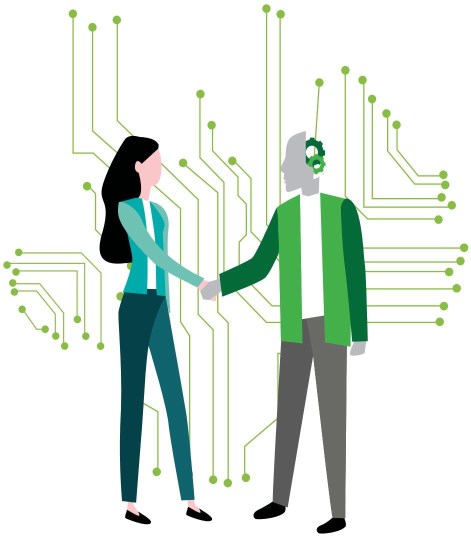
Under the Cyber Academy solution, we offer two programmes:

Enterprise cyber awareness programme

A cyber programme that develops a recognisable awareness campaign, and executes it with the help of a multimedia content package and communication tools. This programme is powered through a world-leading awareness platform covering all functions of an enterprise and a wide range of topics. These topics are important, specialised and practical to gauge the awareness levels of the employees in your enterprise

Tailored awareness programme

To meet the growing needs of the enterprise, we bring in a focused and tailor-made programme based on employee functions and skill levels. These programmes will be delivered through a range of awareness videos, podcasts, mails, presentations, discussions, webinars, and posters. It enables enterprises to monitor, measure and enforce the programme in real-time.



The Cyber Academy enables you to increase the maturity of your enterprise as a whole. This solution:

- Collaborates with the enterprise leadership to embed a security culture for greater resilience
- Alters the security behaviour of employees by increasing their competency and knowledge about threats, risks, and security options to empower them to make better security decisions
- Radically changes the education process to prepare the staff for decisions that align with the enterprise’s security performance objectives and expectations
- Enables users to become a cyber-control via direct behavioural conditioning and by making them cyber aware
- Empowers employees with faster decision-making, resulting in lesser execution time and lower operational expenditures. Controlling the total cost of ownership (TCO) allows the delta savings to be rolled back to meet core business requirements

Step into the realm of the Cyber Mastery Matrix to conquer the unknown

Cyber Experiential Center

Deloitte Cyber Intelligence Center and Knowledge hubs which are present all across the globe, allow you to immerse yourself in a real-world environment and an ideal eco-system. These centers enable and simulate the testing of defense strategies, war-games, attack simulations, and a lot more!

References

1. Michel Cukier, University of Maryland study
2. Worldwide Semiannual Security Spending Guide from International Data Corporation (IDC)
3. 2017 ISSA ESG Survey Results
4. Deloitte Future of Cyber Survey 2019
5. IBM Cost of data breach 2020 report
6. India Cybersecurity Services Landscape report by Data Security Council of India (DSCI).

KEY CONTACTS

ROHIT MAHAJAN
President – Risk Advisory
rmahajan@deloitte.com

ANAND TIWARI
Partner, Risk Advisory
anandtiwari@deloitte.com

AMIT VERMA
Director, Risk Advisory
vermaamit@deloitte.com

REGIONAL CONTACTS

North and East
GAUTAM KAPOOR
Partner, Risk Advisory
gkapoor@deloitte.com

West
ASHISH SHARMA
Partner, Risk Advisory
sashish@deloitte.com

South
GAURAV SHUKLA
Partner, Risk Advisory
shuklagaurav@deloitte.com

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.

Member of Deloitte Touche Tohmatsu Limited