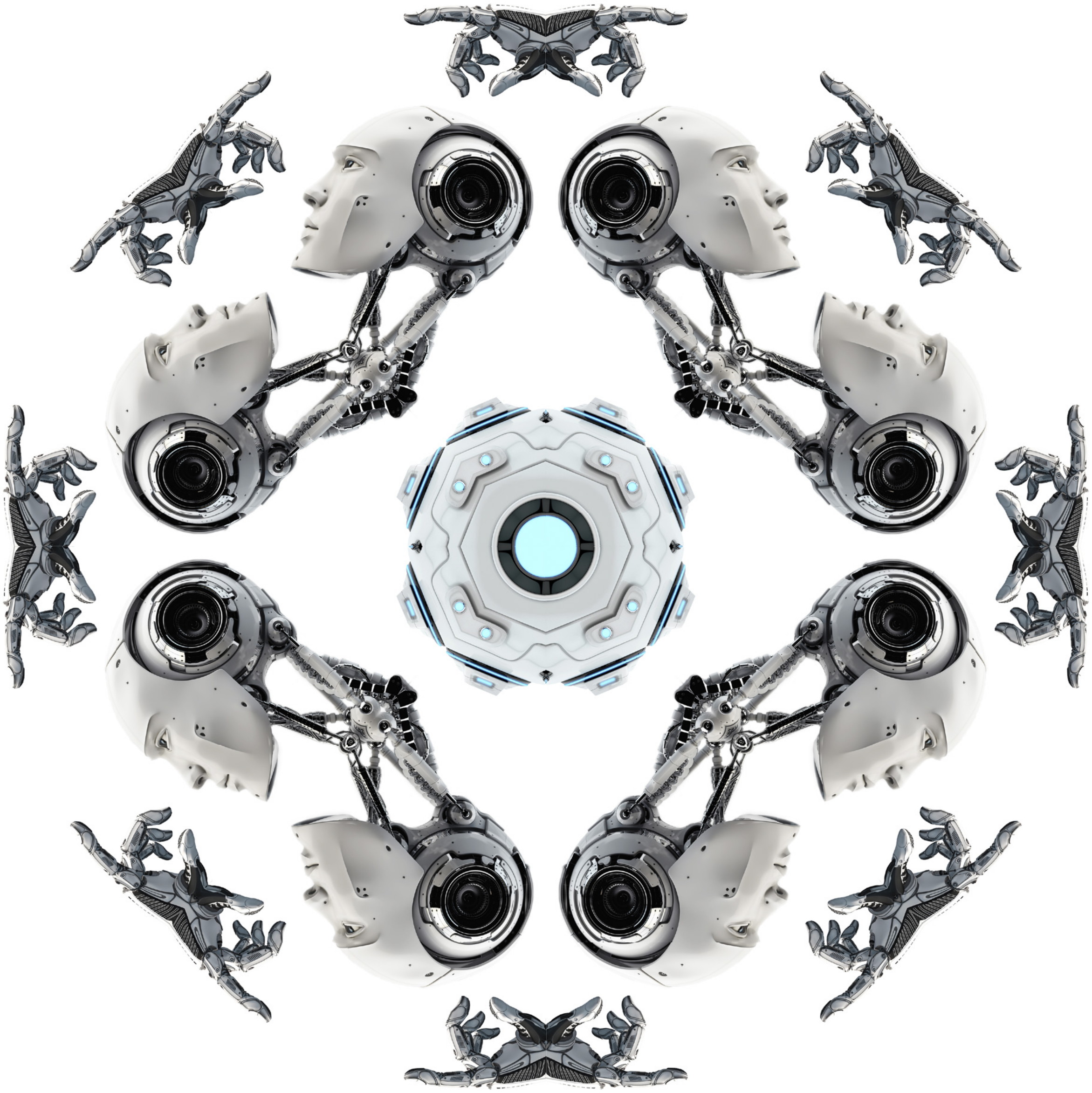
Deloitte.



Smart cyber

How AI can help manage cyber risk

Cyber Risk

Managing cyber risk with smart cyber

In the digital age, artificial intelligence are starting to have the same kind of game-changing impact that factories and assembly lines had on manufacturing at the dawn of the industrial age - dramatically improving efficiency and enabling new products, services, and business models that simply weren't possible before.

Driven by internal and external pressures to continuously evolve and mature their capabilities for mitigating and minimising cyber risk, organisations are actively exploring new technologies and improvement opportunities wherever possible.

Artificial intelligence (AI) is a hot topic in the boardroom and at the watercooler, pushing innovation to new heights in many business areas. Advancements in technologies, processing capabilities, and data availability are enabling computer systems to perform tasks that once required human intelligence to execute. Examples of these include machine learning, natural language processing, speech recognition, computer vision, image comprehension, and robotics.

In cyber security, AI can improve threat intelligence, prediction and protection. It can also enable faster attack detection and response, while reducing the need for human cyber security experts—specialists who are in critically short supply these days.[1] AI can learn from security analysts and improve its performance over time, leading to time savings and better decisions. These "smart cyber" capabilities are urgently needed as cyber attacks continue to grow in volume and sophistication.

Analytics and big data are a key enabler for AI, making it possible to process and analyse vast quantities of data - with parsing, filtering, and visualisation done in near real-time. The adoption of advanced analytics is also a critical step toward becoming an insight-driven organisation.

This report describes how you can use AI to improve your cyber security capabilities and manage cyber risk more efficiently and effectively.

[1] *The changing faces of cyber security: closing the cyber risk gap*, Deloitte, 2018

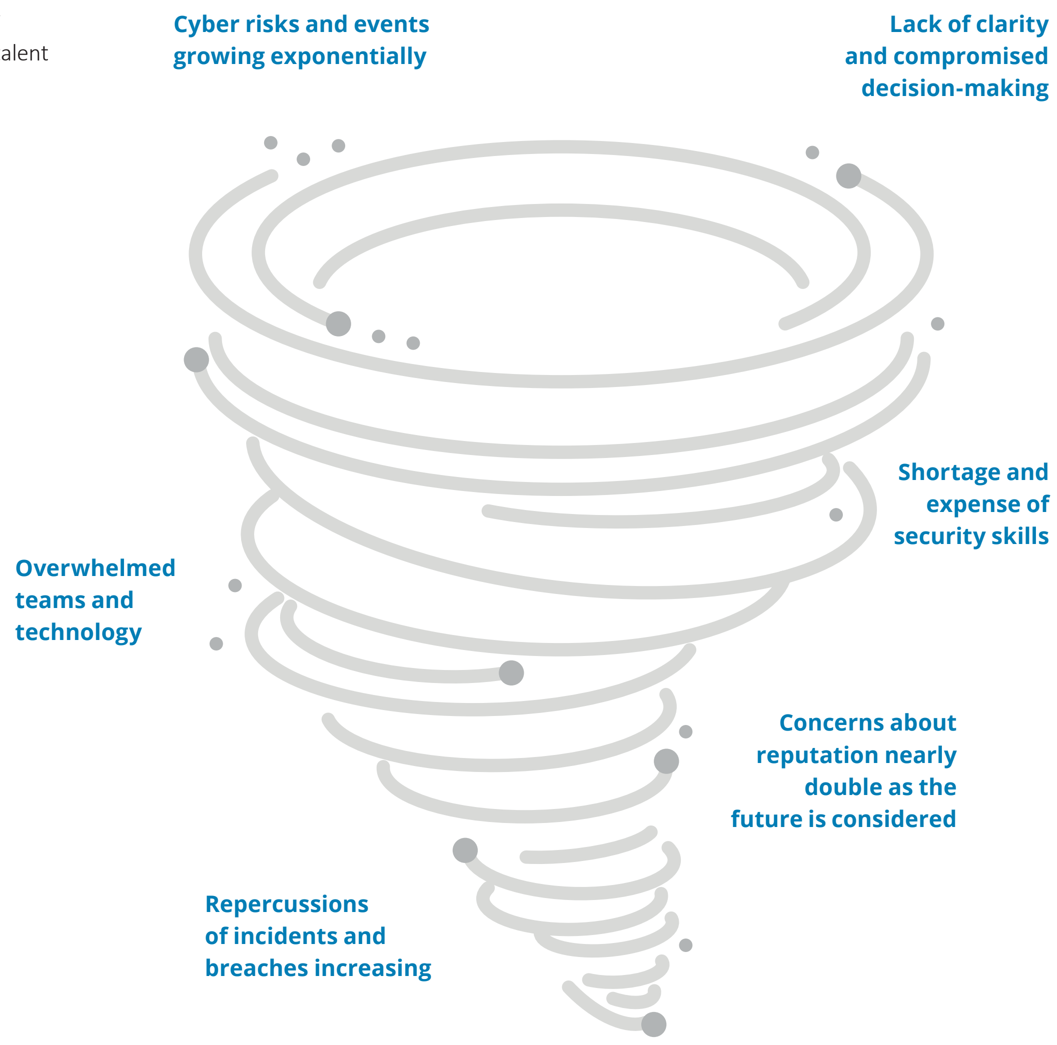
A perfect storm for cyber risk

Cyber security is one of the biggest challenges of the digital age. And it keeps getting bigger.

The cyber threat landscape is growing exponentially. Insider threats actors are learning to evade signature-based systems, and bad actors are using AI to avoid detection by learning the most common detection rules.

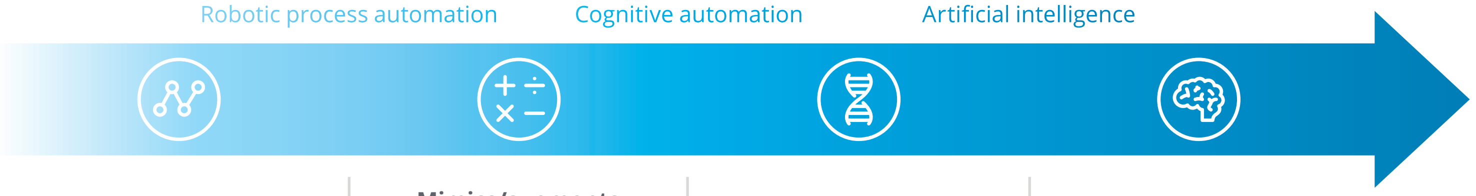
The size and complexity of this growing challenge is overwhelming cyber security teams, while the qualified cyber security talent necessary to successfully fight back is increasingly expensive and hard to find.

With all these forces combined, a perfect storm is forming—but organisations can employ emerging technologies to help them weather the worst.


Cyber risks and events growing exponentially
Lack of clarity and compromised decision-making
Shortage and expense of security skills
Overwhelmed teams and technology
Concerns about reputation nearly double as the future is considered
Repercussions of incidents and breaches increasing

Smart cyber technologies span a broad spectrum, from basic rules-based automation that mimics human action to artificial intelligence that mimics or even surpasses human intelligence and judgment. (Figure 01).

Figure 01: The spectrum of smart cyber technologies



Robotic process automation

Cognitive automation

Artificial intelligence

Mimics human actions

- Used for rules-based processes
- Enables:
  - Faster processing time
  - Higher volumes
  - Fewer errors

Mimics/augments quantitative human judgment

- Used for judgment-based processes
- Capable of:
  - Machine learning
  - Natural language processing
  - Interpretation of human behaviour

Augments human intelligence

- Used for making predictive decisions
- Dynamically self-adapting and self-managing

Mimics human intelligence

- Used for machine intelligence that learns unsupervised, but also communicates and interacts seamlessly with humans (or human associates) as cohorts

Machine learning uses statistical techniques and algorithms that iteratively learn from data, automatically building and improving models without additional programming and user input. This has numerous potential applications in cyber security, such as enabling automated and predictive cyber security capabilities whereby an intelligent software agent could identify an active attack and make the necessary changes to thwart it.

Anomaly detection algorithms in collaboration with Natural language processing (NLP) have many critical applications in cyber security, including the detection and prevention of data leakage. Using behavioural analytics to develop a profile for normal user behaviour for each user, anomaly detection could then monitor for expose abnormal occurrences, while continually learning and inferring from new behaviour patterns.

In the realm of cyber security and cyber risk, current capabilities are most mature on the robotic process automation (RPA) side of the technology spectrum. However, the more sophisticated end (cognitive and artificial intelligence) is rapidly evolving. This is being driven by five main factors:

1. The rising accuracy of predictive algorithms
   Advances in machine learning are improving the ability of predictive risk intelligence to accurately identify emerging risks.
2. The declining costs of technology
   As automation and computing capabilities get faster and cheaper, it's becoming more economical to operationalise predictive risk models.
3. The increasing availability of rich data sources
   Coupled with advances in unstructured data analytics, the availability of rich external and internal data sets is increasing the power and impact of predictive risk intelligence.
4. The growing sophistication of AI technologies
   AI now has the ability to generate its own hypotheses (such as predicting attack techniques) and then provide recommendations to address them.
5. The use of risk management to drive business value
   Risk is an integral part of business; however, gaining the predictive insight to make smarter decisions can be a valuable source of competitive advantage.

According to MIT's Computer Science and Artificial Intelligence Laboratory, the foreseeable future of cyber security will likely revolve around a hybrid approach, with humans and machines working together to manage cyber risk more effectively and efficiently.

Benefits of smart cyber

By applying AI and advanced analytics to vast amounts of internal and external data, smart cyber technologies can generate predictive, usable insights that help you make better cyber security decisions and protect your organisation from threats. They can also help you detect and respond to threats faster by monitoring the cyber environment with a level of speed and accuracy only machines can provide. Perhaps most importantly, smart cyber helps you keep pace with today's endless barrage of increasingly sophisticated cyber attacks.

The traditional layered approach to cyber security is only capable of deterring and detecting the least sophisticated threats. Meanwhile, modern cyber attacks as well as previously identified "modus operandi" of cyber criminals.are being carefully designed to circumvent traditional security controls by learning detection rules. Also, traditional controls may not adequately address insider threats, which are an insidious form of attack from people with legitimate access.

By tapping into a wide range of data sources, smart detection platforms can learn and recognise normal behaviour, develop baselines and detect outliers, identify malicious actions that resemble previously seen events, and make predictions about previously unseen threats. These objectives cannot be achieved with traditional rules- and signature-based controls.

In addition, smart cyber technologies perform tasks in a highly consistent and repeatable way, reducing manual intervention and human errors. This has the extra benefit of making it easier to secure, manage, and audit the cyber environment to achieve compliance with government regulations and other external requirements.

Last but not least, smart cyber technologies can help you make the most of scarce cyber security talent. They enable your cyber teams to get the job done by, first, doing the heavy lifting on routine, labour-intensive tasks so human experts can focus on activities that are more valuable and strategic, and, second, giving cyber specialists the tools to perform at a higher level of competence without requiring years of experience and training.

Key benefits of smart cyber technologies:

- They complement existing security controls and applications in detecting progressive, emerging, and unknown threats.
- They enable enterprises to detect advanced persistent threats and identify indicators of compromise that may go undetected with existing security defences.
- They enhance the threat-hunting process by collecting, correlating, and analysing a wide range of security data.
- They determine threat patterns by tapping into threat intelligence feeds, vulnerability information, device event logs, and contextual data—enabling proactive and predictive security insights.

Getting ahead of risks with predictive risk intelligence

Cyber risk management has typically been a reactive activity, focusing on risks and loss events that have already occurred. But with the rising adoption of advanced analytics and AI technologies, the practice is becoming more forward-looking and predictive.

Predictive risk intelligence uses analytics and AI to provide advance notice of emerging risks, increase awareness of external threats, and improve an organisation's understanding of its risk exposure and potential losses.

Monitoring activities now occur throughout the risk management lifecycle, and can be divided into three categories:

Reactive activities
Capture losses and identify near-miss past events. Develop baseline information to quantify the impact of losses from events. Report on the status of current risks and corrective actions.

Predictive activities
Accumulate and integrate internal and external information to provide reporting and alerts in near real-time. Describe trends and emerging risks. Use reactive and integrated inputs to generate predictive risk insights with advanced analytics.

Integrated activities
Objectively measure risk performance by facilitating the development of key risk indicators, key performance indicators, and associated threshold measures. Enable an accurate description of risk exposure by providing a holistic view across the entire organisation.

How to apply predictive risk intelligence to your organisation

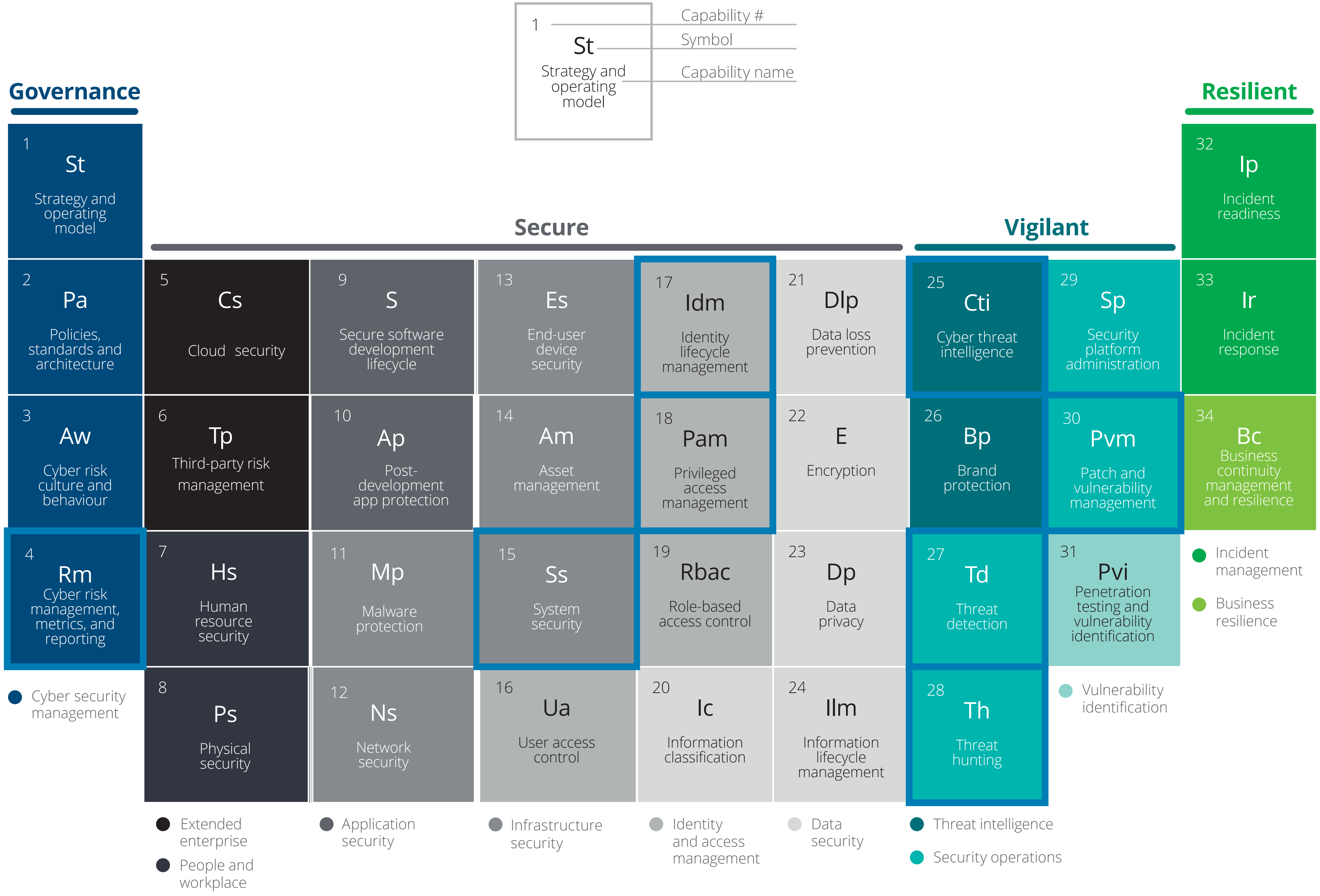
This type of risk intelligence could likely help your organisation in four important cyber security areas:

- **Risk-related decision-making.** Analysing large volumes of contextual data and decision points to determine rational choices, thus helping executives make strategic and financial decisions that align with the organisation's risk appetite (e.g., analysing historical investment data and real-time financial news to make investment decisions; rationally assessing and evaluating asset risks).
- **Risk-sensing.** Identifying or predicting risks that are difficult for humans and rules-based systems to spot, such as new categories of risks, diffused risk signals, or potential sources of future risks (e.g., using data from public forums—such as social media and blogs—where customers, critics, and others gather to discuss and assess an organisation's reputation and related risks).
- **Threat monitoring and detection.** Tracking activities and entities to establish normal behaviour, and detecting sources of anomalies that could create potential risks (e.g., fraud and money-laundering detection; insider-threat detection, including cyber and compliance risks from insiders; real-time cyber threat intelligence).
- **Automation of risk processes.** Automating labour-intensive, error-prone, complex risk processes that deal with high volumes of structured and unstructured data (e.g., third-party due diligence; identity and access management; credit risk management; model risk management)—especially processes that could benefit from a tool that self-learns over time.

Where to start

Many companies are sitting on a wealth of valuable data that's buried beneath a jumble of inefficient and disconnected business processes, making it hard to know where and how to get started. To help you, Deloitte developed a capability-based framework to identify specific areas where AI and cyber analytics can be applied. The framework is depicted as a table that spans all phases of cyber security. (Figure 02).

Some compelling use cases for the blue highlighted elements in automation, AI and analytics are provided on the next page.



1 St Strategy and operating model — Capability # / Symbol / Capability name

Governance
1 St Strategy and operating model
2 Pa Policies, standards and architecture
3 Aw Cyber risk culture and behaviour
4 Rm Cyber risk management, metrics, and reporting
● Cyber security management

Secure
5 Cs Cloud security
6 Tp Third-party risk management
7 Hs Human resource security
8 Ps Physical security
9 S Secure software development lifecycle
10 Ap Post-development app protection
11 Mp Malware protection
12 Ns Network security
13 Es End-user device security
14 Am Asset management
15 Ss System security
16 Ua User access control
17 Idm Identity lifecycle management
18 Pam Privileged access management
19 Rbac Role-based access control
20 Ic Information classification
21 Dlp Data loss prevention
22 E Encryption
23 Dp Data privacy
24 Ilm Information lifecycle management
● Extended enterprise
● People and workplace
● Application security
● Infrastructure security
● Identity and access management
● Data security

Vigilant
25 Cti Cyber threat intelligence
26 Bp Brand protection
27 Td Threat detection
28 Th Threat hunting
29 Sp Security platform administration
30 Pvm Patch and vulnerability management
31 Pvi Penetration testing and vulnerability identification
● Threat intelligence
● Security operations
● Vulnerability identification

Resilient
32 Ip Incident readiness
33 Ir Incident response
34 Bc Business continuity management and resilience
● Incident management
● Business resilience

Figure 02: The periodic table of cyber security elements

The following are some compelling use cases for automation in specific cyber security areas, which may include multiple elements in the table.

4
Rm
Cyber risk management, metrics, and reporting

Governance, risk, and compliance

Governance and risk management
Informs overall strategy and improves reporting capabilities by using large volumes of contextual data and decision points to help with strategic decision-making that aligns with the organisation's risk appetite.

Regulation synthesis and mapping
Develops and maintains an organisation's integrated security controls framework, extracting information from multiple regulatory data sources and guidelines.

Assessment triggering
Conducts automated assessments periodically, or is triggered automatically by changes to applications and/or business processes.

KRI automation
Automates the collection and visualisation of key risk indicator metrics to enable the organisation to assess and address risk exposure.

Responsibility allocation
Uses self-service processes to allocate cyber security responsibilities across teams, improving efficiency and enabling closer alignment with risk owners.

Control testing
Automates control testing so that it continually assesses control effectiveness and provides near real-time updates about the organisation's security posture.

17
Idm
Identity lifecycle management

18
Pam
Privileged access management

Identity and access management (IAM)

Role maintenance
Uses an AI engine to provide recommendations on role maintenance, helping organisations streamline the difficult, costly, and time-consuming task of keeping role definitions up-to-date.

Role mining engine
Extends the role maintenance engine to mine roles from multiple data sources, recommending new roles and entitlements.

Access request recommendation engine
Makes the access request process simpler by analysing various data sources—such as peer group access and historical access requests—and then recommending the level of access required for a user.

Access certification analytics Analyses different data sets and applies analytics to improve the certification process by: pre-approving certification items based on access request data, detecting anomalies in the attestation cycle, and using peer group data to calculate a confidence score that helps reviewers make informed decisions.

Access usage data for analytics engine
Incorporates access usage data into the analytics engine to help it generate more informed and efficient insights.

At the more sophisticated end of the technology spectrum, the following are some of the many potential uses for AI and analytics technologies in cyber security.

15
Ss
System security

System security

Control effectiveness
Augments and assesses the effectiveness of tried and tested tools such as firewalls, proxies, and data leak prevention solutions by monitoring the available log data and then identifying and remediating misconfigurations.

25
Cti
Cyber threat intelligence

Cyber threat intelligence

Cyber risk sensing
Identifies or predicts risks that are often difficult for humans and rules-based systems to detect, including new categories of risks, diffused risk signals, and potential sources of future risks such as increased use of social media.

27
Td
Threat detection

Threat detection

Anomalous behaviour detection
Helps identify anomalous data access activity and malicious application activity by focusing on user logins, changes in user behaviour, and unapproved changes.

Threat discovery
Monitors activities and entities to establish normal behaviour, and detects sources of anomalies that could create potential risks such as fraud, money laundering, and insider threats.

Alert cleansing and prioritisation Uses machine learning to significantly automate the first level of triage based on factors such as type of attack, frequency and previous experience.

Targeted investigation and support Uses machine learning and advanced analytics to drive new insights through historical analysis, thereby allowing investigations into incidents based on current and historical data to be done quickly and efficiently.

28
Th
Threat hunting

30
Pvm
Patch and vulnerability management

Threat hunting and vulnerability management

Threat hunting
Quickly searches for new threats by importing known tactics, techniques, procedures, and attack patterns—along with vulnerability details and remediation information—to help neutralise threats early in the attack cycle.

Vulnerability scanning
Uses software robots (bots) to initiate and scan applications, systems, and other assets for vulnerabilities, assessing risk and prioritising the patch schedule.

Configuration review
Uses bots to review system configurations to ensure baseline hardening is applied and ensure no misconfigurations.

Attack-path modelling
Performs predictive analytics on security data to determine vulnerable entry points and the likely path an attacker might use to gain access.

From promise to practice

AI has been receiving a lot of focus lately. Now it's time to move from talk to action. Here are seven steps you can start taking today to boost your organisation's cyber security capabilities through the use of AI technologies and analytics.

1

Embrace the future Collaborate within your ecosystem to help shape the future of these powerful new cyber technologies. Enabling your organisation to leverage the power of data, analytics and AI to become a truly insights driven organisaion

2

Educate yourself and your teams Understand the business opportunities associated with AI technologies and analytics in cyber security, immersing yourself in internal forums and decision-making processes to ensure that you are a valuable contributor.

3

Reassess the risk and threat landscape Understand the impact of new technologies and develop appropriate risk management responses.

4

Redefine your accountability model Consider how changes in the operating environment will affect the risk landscape and required controls, and then adjust your cyber security team's roles and responsibilities accordingly.

5

Rationalise your control framework Encourage risk-intelligent design for new systems, technologies, and control frameworks to reduce unnecessary control layers and build more preventative and automated capabilities up front.

6

Start small and scale fast Develop a practical strategy for applying AI technologies and analytics to cyber security by identifying opportunities with high impact, low complexity, readily available data, and insufficient current capabilities.

7

Rethink your cyber security talent strategy Update your talent strategy, taking steps to ensure highly skilled cyber security professionals are leading the way on your cyber security efforts.

AI and analytics can lift your company's cyber security capabilities to the next level. By taking the lead on applying these disruptive innovations to cyber security, you can tip the balance in your favour and stay a step ahead of the threats.

Cyber Risk Contacts

Southern Africa

Navin Sing
Managing Director:
Risk Advisory Africa
+27 83 304 4225
navising@deloitte.co.za

Shahil Kanjee
Director: Risk Advisory Africa
Cyber Risk Leader
+27 83 634 4445
skanjee@deloitte.co.za

Tiaan Van Schalkwyk
Associate Director:
Risk Advisory Southern Africa
+27 83 475 3551
tvanschalkwyk@deloitte.co.za

Eric Mc Gee
Associate Director:
Risk Advisory Southern Africa
+27 82 872 9607
erimcgee@deloitte.co.za

Catherine Stretton
Director: Risk Advisory Africa
Digital Leader
+27 84 444 7033
cstretton@deloitte.co.za

Wessel Oosthuizen
Associate Director: Risk Advisory Africa
AI Leader
+27 84 307 0664
woosthuizen@deloitte.co.za

East Africa

Julie Akinyi Nyangaya
Risk Advisory Regional Leader:
East Africa
+254 72 011 1888
jnyangaya@deloitte.co.ke

Urvi Patel
Director: Risk Advisory
East Africa
+254 71 405 6887
ubpatel@deloitte.co.ke

West Africa

Anthony Olukoju
Risk Advisory Regional Leader:
West Africa
+234 805 209 0501
aolukoju@deloitte.com.ng

Temitope Aladenusi
Director: Risk Advisory
West Africa
+234 805 901 6630
taladenusi@deloitte.com.ng

Central Africa

Tricha Simon
Risk Advisory Regional Leader:
Central Africa
+263 867 700 0261
tsimon@deloitte.co.zm

Rodney Dean
Director: Risk Advisory
Central Africa
+263 867 700 0261
rdean@deloitte.co.zm

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 286,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your 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 who relies on this communication.