

Smart cyber

How AI can help manage cyber risk

Cyber Risk 



Managing cyber risk with smart cyber

In the digital age, artificial intelligence technologies 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 minimizing cyber risk, organizations 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 AI 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, AI technologies can improve threat intelligence, prediction, and protection. It can also enable faster attack

detection and response, while reducing the need for human cybersecurity 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 analyze vast quantities of data—with parsing, filtering, and visualization done in near real-time. The adoption of advanced analytics is also a critical step toward becoming an insight-driven organization.

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

1. *The changing faces of cybersecurity: closing the cyber risk gap*, Deloitte, 2018

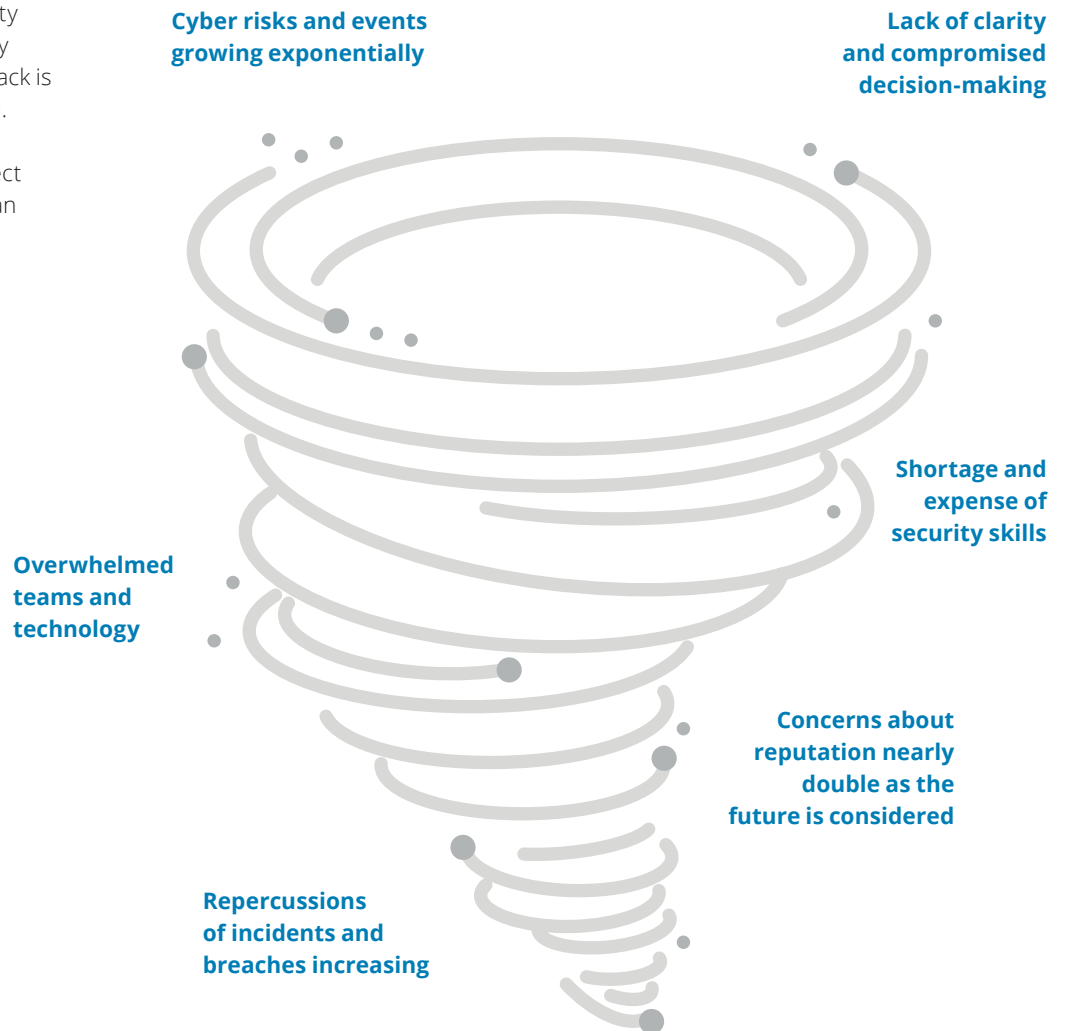
A perfect storm for cyber risk

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

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

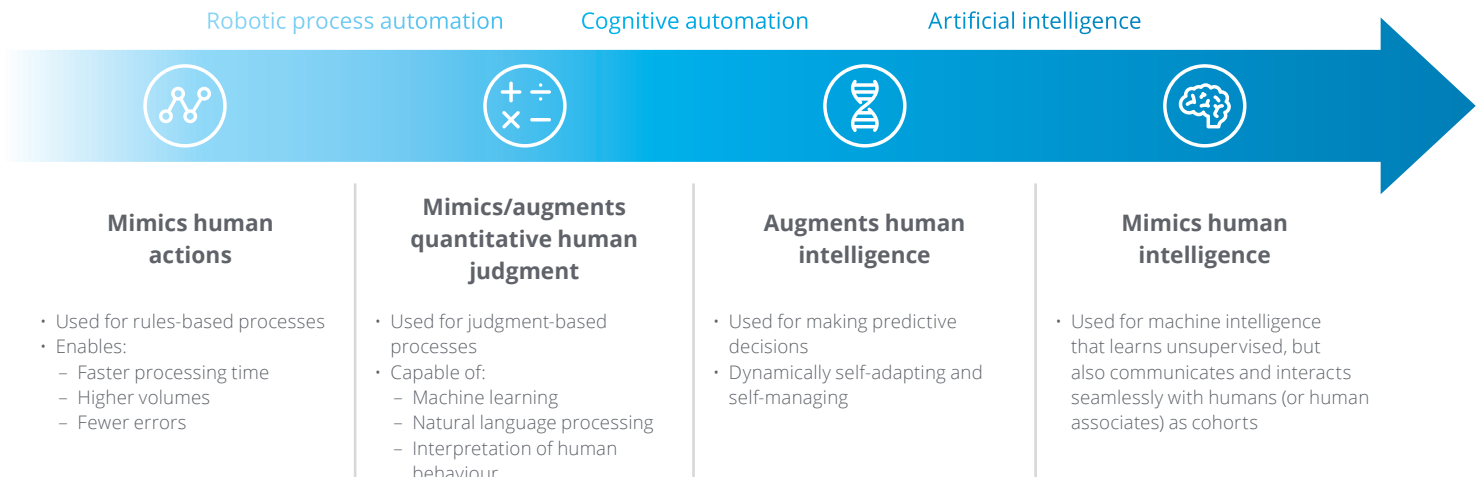
The size and complexity of this growing challenge is overwhelming cybersecurity teams, while the qualified cybersecurity talent necessary to successfully fight back is increasingly expensive and hard to find.

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



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

Figure 01: The spectrum of smart cyber technologies



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

Natural language processing (NLP) also has many critical applications in cybersecurity, including the prevention of data leakage. Using behavioural analytics to create baseline markers of normal user behaviour, NLP could develop a profile for each user and then monitor for abnormal occurrences while continually learning and inferring from new behaviour patterns.

In the realm of cybersecurity 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 operationalize 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 cybersecurity 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 decisions and protect your organization 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 important, smart cyber helps you keep pace with today's endless barrage of increasingly sophisticated attacks.

The traditional layered approach to cybersecurity is only capable of deterring and detecting the least sophisticated threats. Meanwhile, modern cyberattacks 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 recognize 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 cybersecurity **talent**. They enable your cyber teams to get the job done with fewer resources 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 high level 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 analyzing 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 in front 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 organization'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 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 organization.

How to apply predictive risk intelligence to your organization

This type of risk intelligence could likely help your organization in four important cybersecurity areas:

- **Risk-related decision-making.** Analyzing large volumes of contextual data and decision points to determine rational choices, thus helping executives make strategic and financial decisions that align with the organization's risk appetite (e.g., analyzing 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 organization'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 technologies and cyber analytics can be applied. The framework is depicted as a table that spans all phases of cybersecurity. (Figure 02).

Governance

1 St Strategy and operating model		
2 Pa Policies, standards and architecture	5 Cs Cloud security	9 S Secure software development lifecycle
3 Aw Cyber risk culture and behaviour	6 Tp Third-party risk management	10 Ap Post-development app protection
4 Rm Cyber risk management, metrics, and reporting	7 Hs Human resource security	11 Mp Malware protection
	8 Ps Physical security	12 Ns Network security

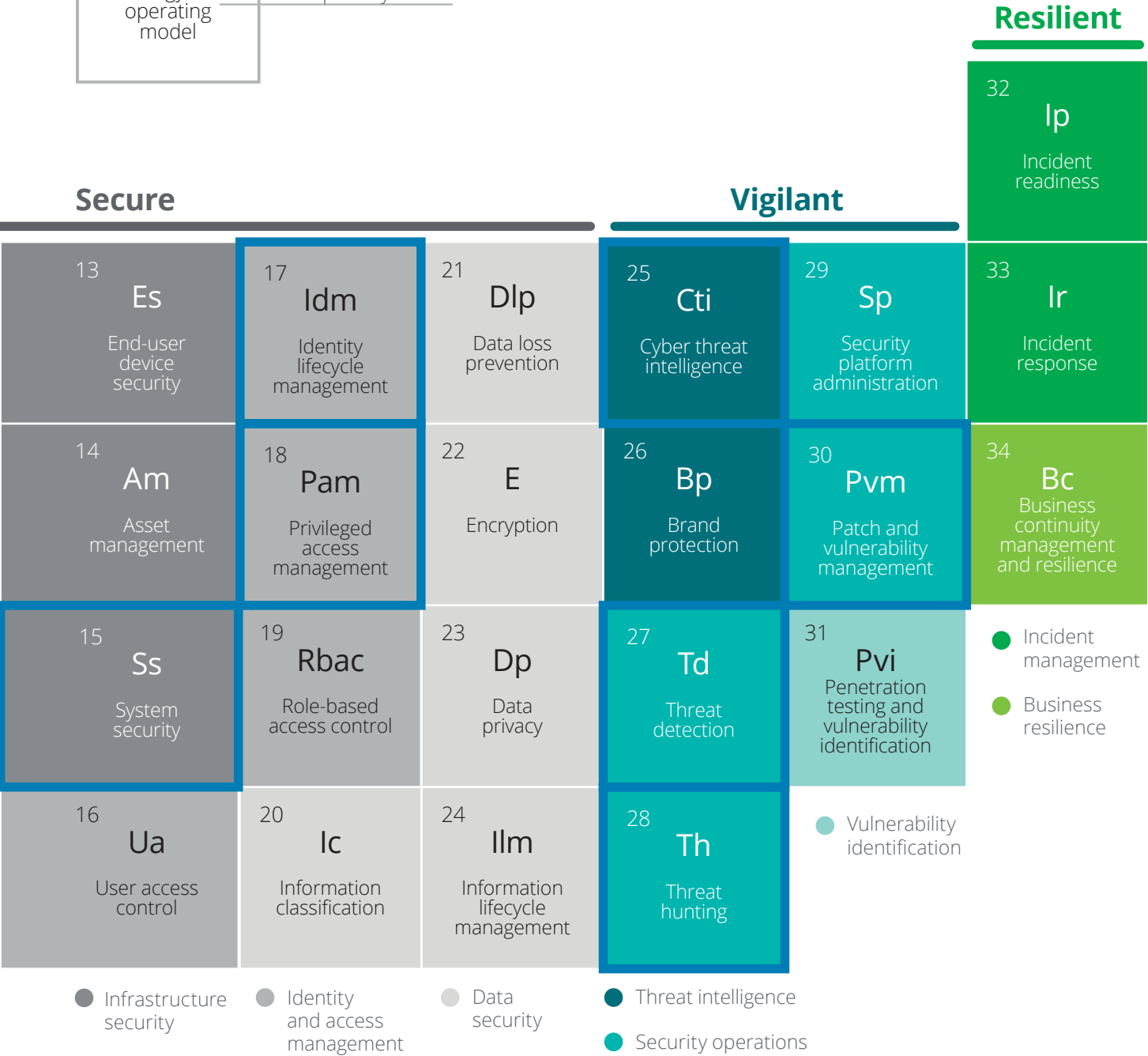
● Cybersecurity management

- Extended enterprise
- People and workplace

● Application security

Figure 02: The periodic table of cybersecurity elements

1	Capability #
St	Symbol
Strategy and operating model	Capability name



The following are some compelling use cases for **automation** in specific cybersecurity 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 organization's risk appetite.

Regulation synthesis and mapping
Develops and maintains an organization's integrated security controls framework, extracting information from multiple regulatory 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 visualization of key risk indicator metrics to enable the organization to assess and address risk exposure.

Responsibility allocation
Uses self-service processes to allocate cybersecurity 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 organization's security posture.

17
Idm
Identity lifecycle management

Identity and access management (IAM)

Role maintenance
Uses an AI engine to provide recommendations on role maintenance, helping organizations 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 analyzing 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
Analyzes 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.

18
Pam
Privileged access management

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

15

Ss

System security

System security

Control effectiveness

Augments and assesses the effectiveness of tried and tested tools such as firewalls, proxies, and data loss 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 prioritization

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 a big data platform 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

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 neutralize threats early in the attack cycle.

Vulnerability scanning

Uses bots to initiate and scan applications, systems, and other assets for vulnerabilities, assessing risk and prioritizing the patch schedule.

Configuration review

Uses bots to review system configurations to ensure baseline hardening 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.

30

Pvm

Patch and vulnerability management

From promise to practice

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



1

Embrace the future

Collaborate with your ecosystem to help shape the future of these powerful new cyber technologies.

2

Educate yourself and your teams

Understand the business opportunities associated with AI technologies and analytics in cyber, immersing yourself in internal forums and decision-making processes to ensure 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 team's roles and responsibilities accordingly.

5

Rationalize 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 cybersecurity by identifying opportunities with high impact, low complexity, readily available data, and insufficient current capabilities.

7

Rethink your cyber talent strategy

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

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

Contacts



Nick Galletto

Global and Canadian Cyber Risk Services Leader
ngalletto@deloitte.ca
416-601-6734



Marc MacKinnon

National Cyber Strategy Leader
mmackinnon@deloitte.ca
416-601-5993



Dina Kamal

Cyber Artificial Intelligence Leader, Omnia
dkamal@deloitte.ca
416-775-7414



Beth Dewitt

National Cyber Secure Leader
bdewitt@deloitte.ca
416-643-8223



Rocco Galletto

National Cyber Vigilant Leader
rgalletto@deloitte.ca
416-643-8718



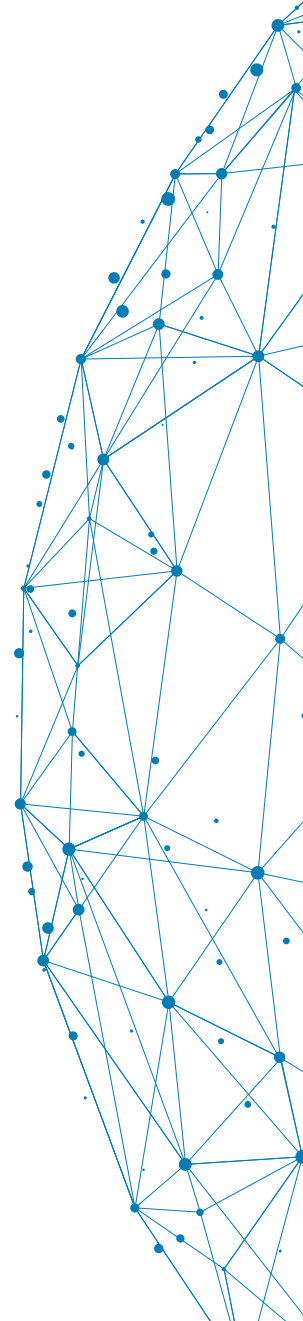
Kevvie Fowler

National Cyber Resilient Leader
kfowler@deloitte.ca
416-867-8149



Paul Hanley

National Cyber Innovation Leader
phanley@deloitte.ca
416-956-9090







www.deloitte.ca

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights and service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 264,000 professionals—9,400 of whom are based in Canada—make an impact that matters, please connect with us on LinkedIn, Twitter or Facebook.

Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

© Deloitte LLP and affiliated entities.

Designed and produced by the Deloitte Design Studio, Canada. 18-5679M