Capgemini
RESEARCH INSTITUTE

Reinventing Cybersecurity with Artificial Intelligence

The new frontier in digital security

Executive Summary – key takeaways

Bolstering cybersecurity with AI has become an imperative for organizations

- Organizations are counting on AI to help overwhelmed cybersecurity analysts.
- Nearly two-thirds think that AI will help identify critical threats.
- Sixty-nine percent of organizations believe AI will be necessary to respond to cyberattacks.
- AI-enabled response to cyber threats is the new frontier for cybersecurity as hackers are already using AI for cybersecurity attacks.

The pace of adoption of AI in cybersecurity is picking up

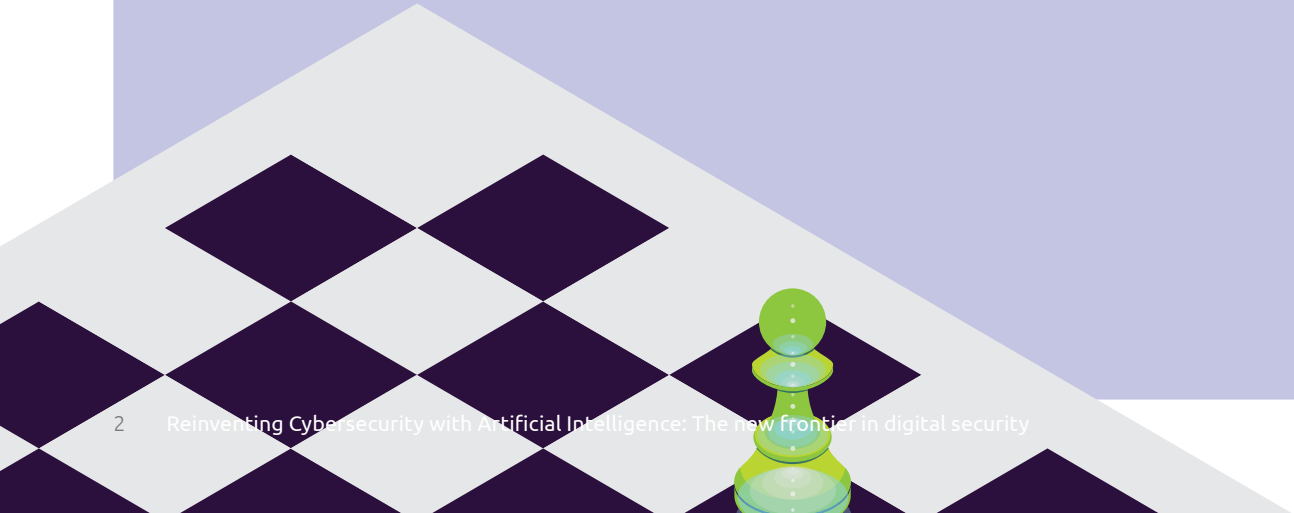
- Nearly one in five organizations used AI pre-2019. However, adoption is poised to skyrocket, with almost two out of three organizations planning to employ AI by 2020.

There is a compelling business case for using AI in cybersecurity

- Three out of four executives say that using AI allows their organization to respond faster to breaches.
- Three in five firms say that using AI improves the accuracy and efficiency of cyber analysts.
- A majority of organizations say that AI lowers the cost of detecting and responding to breaches by 12%, on average.

Building a roadmap for implementing AI in cybersecurity

- **Identify data sources and create data platforms to operationalize AI** – Buying or building a data platform to provide a consolidated view of data should be a first step for organizations that want to use AI in cybersecurity successfully.
- **Select the right use cases to accelerate and maximize benefits** – We identified 5 use cases with the highest benefit and the lowest implementation complexity: malware detection, intrusion detection, scoring risk in the network for operational technology (OT), fraud detection for information technology (IT), and user/machine behavioral analysis for the internet of things (IoT).
- **Collaborate externally to enhance threat intelligence** – Collaboration via crowd-sourced platforms ensures your organization keeps up to speed with the threats facing other security professionals; it also plays an important part in improving the logic of AI algorithms so that they detect threats efficiently.
- **Deploy security, orchestration, automation, and response ('SOAR') to improve security management** – SOAR makes the use of AI more effective and impactful by enabling rapid response to detected threats.
- **Train cyber analysts to be AI-ready** - Teams need knowledge of key processes within an organization to ensure the AI algorithm can close potential threat entry points.
- **Install governance for AI in cybersecurity to deliver long-term improvement** – Governance is essential to ensure the AI produces the expected outcomes and that the AI has not been compromised.



Introduction

Artificial intelligence (AI) has already been deployed in a multitude of applications to increase productivity, improve sales or enhance experiences. However, one crucial, though often overlooked AI application, is the focus of this report – enhancing protection against cyberattacks.

When used in conjunction with traditional methods, AI is a powerful tool for protecting against cybersecurity attacks. In the Internet Age, with hackers' ability to commit theft or cause harm remotely, shielding assets and operations from those who intend harm has become more difficult than ever. The numbers are staggering – Cisco alone reported that, in 2018, they blocked seven trillion threats on behalf of their customers.[1]

With such ever-increasing threats, organizations need help. Some organizations are turning to AI, not so much to completely solve their problems (yet), but rather to shore up their defenses. As Martin Borrett, IBM distinguished engineer, chief technology officer and technical executive for IBM's European security business unit says, "Organizations are looking for automation, machine learning, AI to help make cybersecurity more manageable, more efficient, more effective and lower their risk."

To better understand the cybersecurity challenges organizations face and explain how AI is helping to overcome them, we surveyed 850 senior executives from IT Information Security, Cybersecurity and IT Operations in seven sectors across 10 countries. We also conducted in-depth interviews with industry experts and academics. Finally, we analyzed 20 use cases of AI in cybersecurity spread across IT (information technology), OT (operational technology), and IoT (internet of things) to understand the benefits, complexities, and levels of implementation of these use cases in organizations. This report analyzes organizations that have already deployed cybersecurity solutions using AI or are planning to do so in the next year.

In the report we explore:

- Why AI-enabled cybersecurity is increasingly necessary
- How organizations are benefitting from AI in cybersecurity
- Where organizations should focus their cybersecurity initiatives
- Building a roadmap for implementing AI in cybersecurity

AI in cybersecurity: definitions

- **Artificial intelligence (AI):** Artificial intelligence (AI) is a collective term for the capabilities shown by learning systems that are perceived by humans as representing intelligence. Today, typical AI capabilities include speech, image and video recognition, autonomous objects, natural language processing, conversational agents, prescriptive modeling, augmented creativity, smart automation, advanced simulation, as well as complex analytics and predictions.
- **Machine learning (ML):** Machine learning is the science of getting computers to act without being explicitly programmed*.
- **Deep learning (DL):** Algorithms inspired by the structure and function of the brain, creating an artificial neural network.
- **AI in cybersecurity:** a set of capabilities that allows organizations to detect, predict and respond to cyberthreats in real time using machine and deep learning.

For this research, we are considering the use of AI embedded in security products as well as cyber systems that are based on proprietary/ in-house AI algorithms modified to suit organizational requirements. In this report, AI is used as an umbrella term that includes machine learning and deep learning techniques/technologies.

(Source: Andrew Ng, Stanford University)

AI-enabled cybersecurity is increasingly necessary

Organizations face an urgent need to continually ramp up and improve their cybersecurity. This is because the number of end-user devices, networks, and user interfaces continues to grow as a result of advances in cloud, the IoT, 5G and conversational interfaces. John Meakin, interim CISO of GlaxoSmithKline (GSK), says that threat levels are on the rise. "We have seen a gradual but steady increase in threat levels," he says. "This is represented by definable attempts at intrusion or information theft, with the occasional apparent service continuity attack."

Today, even hackers use AI effectively. For example, AI algorithms are more successful at sending 'spear phishing' tweets (personalized tweets sent to targeted users to trick them into sharing sensitive information). AI can send the tweets six times faster than a human and with twice the success.[2] With the enlargement of attack surface and the increased sophistication of attacks, AI in cybersecurity is becoming a key weapon to thwart cyber-attacks.

Organizations are turning to AI as threats overwhelm cyber analysts

Global business internet traffic is expected to increase three-fold from 2017 to 2022[3]. Cyber analysts are finding it increasingly difficult to effectively monitor current levels of data volume, velocity, and variety across firewalls. Signature-based cybersecurity solutions are unlikely to deliver the requisite performance to detect new attack vectors. In fact, our data shows that 61% of organizations acknowledge that they will not be able to identify critical threats without AI. The increases in cyber attacks that can quickly compromise critical operations within an enterprise also require enhanced capabilities that can best be provided through AI. "I suspect that organizations are turning to AI in order to try to solve those problems that they can't buy a box for," says Paul Owen, head of cybersecurity innovation, Department of Works and Pensions (DWP), UK.

We asked organizations about the vast array of data points, cloud infrastructure, and end-point devices they must track to detect and prevent intrusion:

- Over half (56%) say their cybersecurity analysts are overwhelmed
- Close to a quarter (23%) are not able to successfully investigate all identified incidents.

This is critical, because if cyber analysts are not able to track anomalies, more incidents and breaches will follow.

The type of cyber-attacks that require immediate intervention, or that cannot be remediated quickly enough by cyber analysts, have notably increased. We asked executives to report on cybersecurity incidents through time-sensitive applications (i.e., applications where impacts can be severe if threats are not resolved very quickly, such as hacked control of an automobile or airplane):

- 42% reported an increase in incidents through time-sensitive applications
- The average increase in these types of incidents was estimated at 16%.

In one case, a hacker was able to access the GPS tracker apps of 27,000 vehicles. This gave them the ability to shut down the engines of these vehicles, even when they were in motion.[4]

We also inquired about cybersecurity incidents through machine-speed attacks (ransomware and other automated attacks that propagate and/or mutate very quickly and are virtually impossible to neutralize using human-dependent response mechanisms):

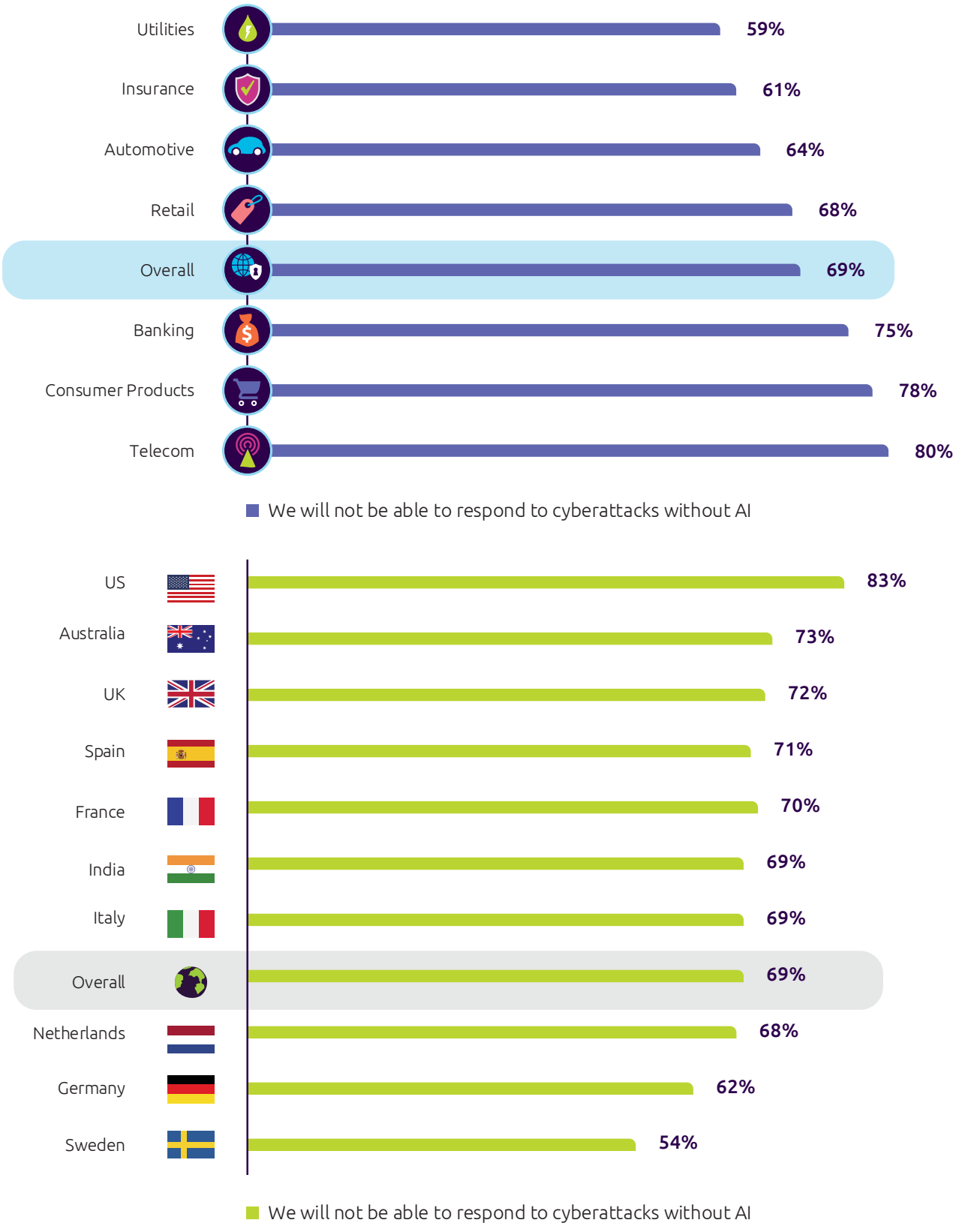
- 43% of executives noted an increase in machine-speed attacks
- The average increase in machine-speed attacks was estimated to be 15%.

In this environment, organizations accept and understand the magnitude of the effort required to secure themselves from cyberattacks. As Figure 1 shows, 69% of organizations believe that they will not be able to respond to cyberattacks without AI.

Our research indicates that firms are reacting to this new reality and are responding accordingly by increasing investment in AI-based solutions:

- Close to half (48%) said that budgets for AI in cybersecurity will increase by an average of 29% in FY2020.
- The average increase in FY2020 budgets for nearly one in ten organizations will be more than 40% over FY2019 budgets.

Figure 1: **Organizations are counting on AI to help identify threats and thwart attacks**



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

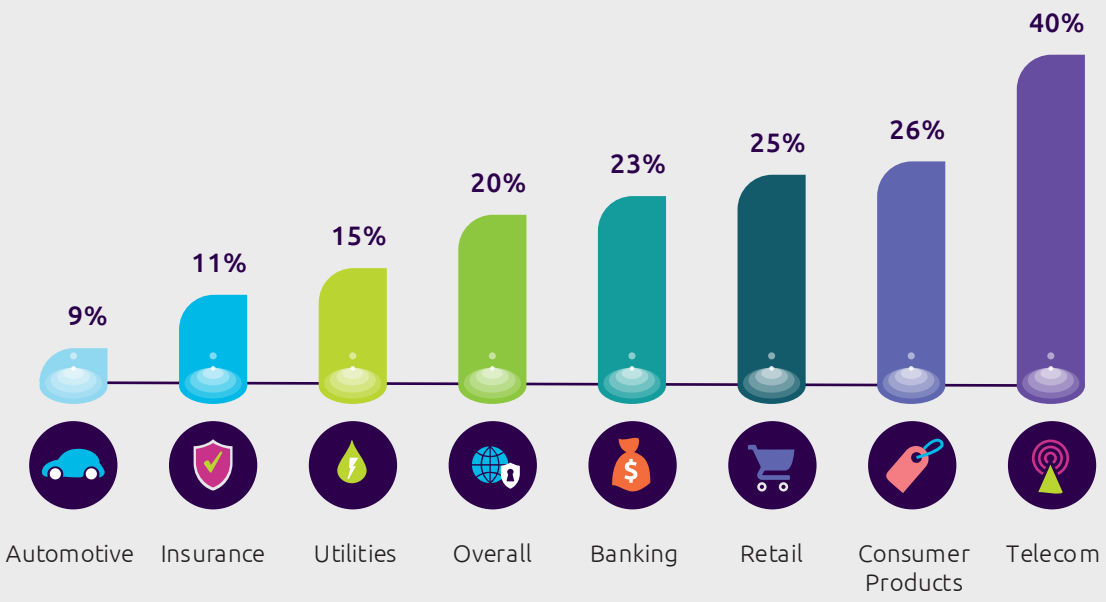
Widespread cybersecurity breaches

As businesses evolve and grow, so too does the threat of cyberattacks. One in five executives (21%) said that their organization experienced a cybersecurity breach leading to unauthorized access (to networks, devices, applications or data) in 2018. In addition, over the next twelve months, 14% expect the number of cyberattacks to as much as double.

Organizations pay a heavy price for cybersecurity breaches: 20% report losses of more than $50 million. Telecom firms, for example, high huge amounts of customer data, which make them an ideal target for cyberattacks. Forty percent of these firms reported financial damage of more than $50 million due to cybersecurity breaches.

The telecom industry has the highest reported incidence of losses exceeding $50 million

What was the approximate financial damage to your organization in $ million resulting from the cybersecurity breach?-More than $50 million



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N=850 executives

Over a third (35%) of firms said that critical operations (such as website/apps or factory/power grid) were impacted by cybersecurity breaches. In one such instance, a leading Japanese manufacturer suffered an attack that led to a partial shutdown of its production lines for three days, dropping production output by 50%.

Cyber-attacks via the latest digital technologies on the rise

The newest digital mediums are increasing the attack surface for hackers to exploit. Executives point out that cyber-attacks through these digital mediums have increased over the past two years:

- Around half (49%) say cybersecurity incidents through cloud services (e.g. public cloud server instance is configured in a format that makes them vulnerable to breaches) have increased by 17%.
- Forty-two percent of executives report that cybersecurity incidents through IoT devices (e.g. hackers infiltrate unsecured IoT devices for DDoS attacks) have increased, with the average increase being 16%.

Organizations are increasing the pace of adoption of AI in cybersecurity

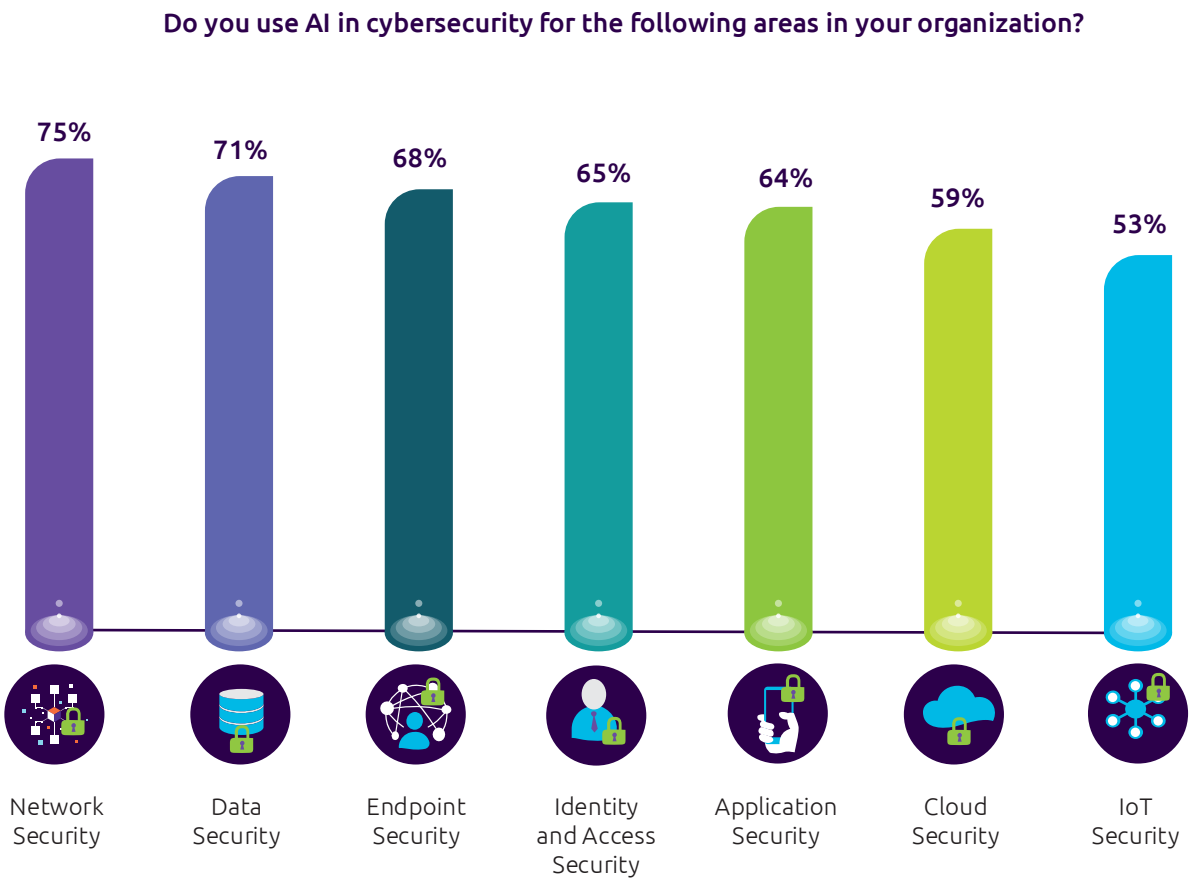
The use of AI in cybersecurity is gathering pace:

- Overall, close to three-quarters of firms (73%) said they were testing use cases for AI for cybersecurity in some way.
- Currently, 28% are using security products with AI embedded, with 30% using proprietary AI algorithms. The remainder, 42%, currently either use (or plan to use by next year) both proprietary solutions and embedded products.

Under the AI umbrella, the use of machine and deep learning in cybersecurity has been trending upward. Nearly one in five organizations used AI pre-2019. However, adoption is poised to skyrocket, with almost two out of three (63%) organizations planning to employ AI by 2020.

We asked executives where they are using AI in cybersecurity in their organizations. The number one application was for network security, followed by data security and endpoint security. Since the network is the backbone of any IT system, it is not surprising to see the latest technology – AI – deployed to protect it. Data, a valuable commodity prized by hackers, requires protection like any other asset. And the presence of endpoint security in third place is indicative of the proliferation of endpoint devices, which are expected to increase to over 25 billion devices by 2021.[5]

Figure 2: **Network Security has the highest deployment of AI in cybersecurity**



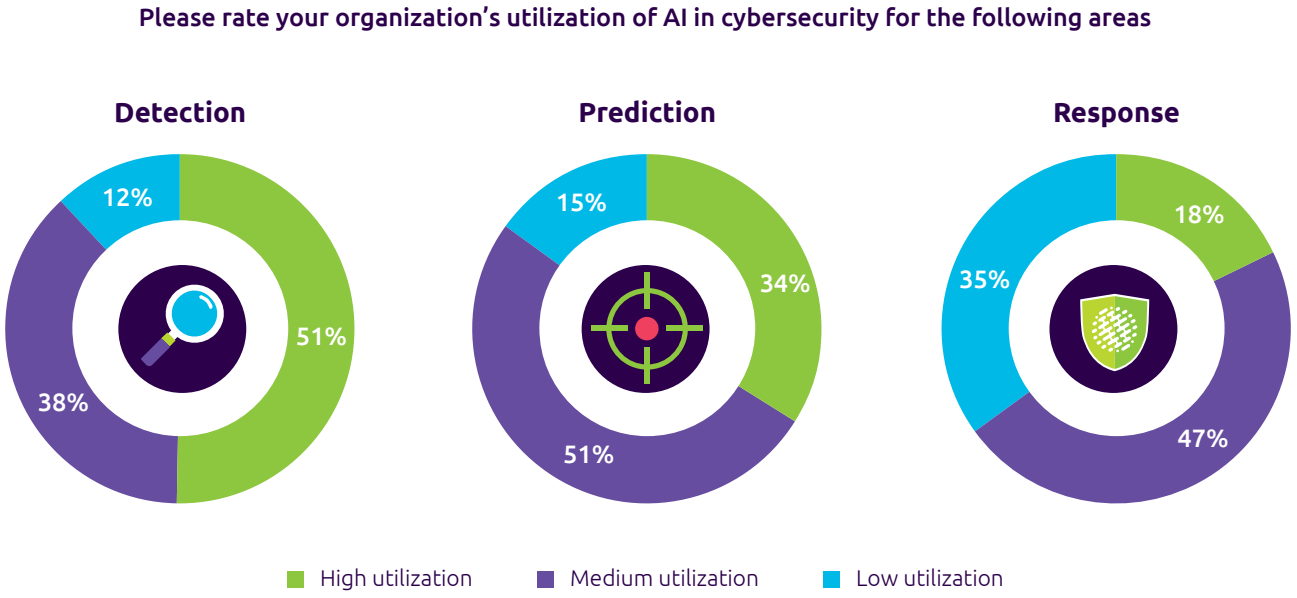
Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

With network traffic increasing exponentially, it is a growing challenge for cyber analysts to identify deviations in patterns of behavior. AI and ML make it easier to analyze these patterns and identify potential anomalies quickly. AT&T is using machine learning to detect new patterns in network traffic and to indicate bad actors that can cause network disruptions or data breaches.[6] "I see more than 100 billion potential vulnerability scans and probes across our global backbone every single day," says Bill O'Hern, senior vice president and chief security officer at AT&T. Referring to device connectivity (internet of things), software-defined networks and 5G, he adds, "You can't really protect these new technologies with a legacy approach. It's really key to understand that you need to evolve your capability along with these technologies and take advantage of machine learning or other AI technologies in harmony as a platform across your whole ecosystem."[7]

Similarly, Sunsweet, one of the world's largest dried-fruit manufacturers, has deployed a machine learning technology that studies the behavior of every user and device in its overall network. The aim is to provide complete visibility of its ecosystem and to detect any possible intrusion or anomaly. According to Terrell Johnson, manager of Systems and Networks, Sunsweet, this delivers significant benefits. "The amount of visibility we achieve from its (the technology's) machine learning approach is unmatched," he explains. "We are now finding anomalies, in real-time, that would have taken us weeks, or even months, to find on our own."[8]

We asked executives about how they are utilizing AI to address cyber threats across three categories: detection, prediction and response. While more than half of the executives surveyed say they make extensive use of AI in cyberthreat detection, only 34% use it extensively for prediction, followed by 18% for response.

Figure 3: Higher utilization of AI for detection than prediction or response



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

Detection: AI is used extensively to detect cyber threats. This reflects the unique capabilities of these technologies: machine learning or deep learning-based detection allows organizations to continuously evolve detection parameters, using behavioral analysis to identify anomalies. Honeywell, for example, has introduced an AI solution to defend industrials against attacks intended to disrupt operations. Their secure media exchange (SMX) detects threats introduced via USB devices, such as flash drives and charge cables. USB devices remain the primary attack vector in industrial control systems.[9]

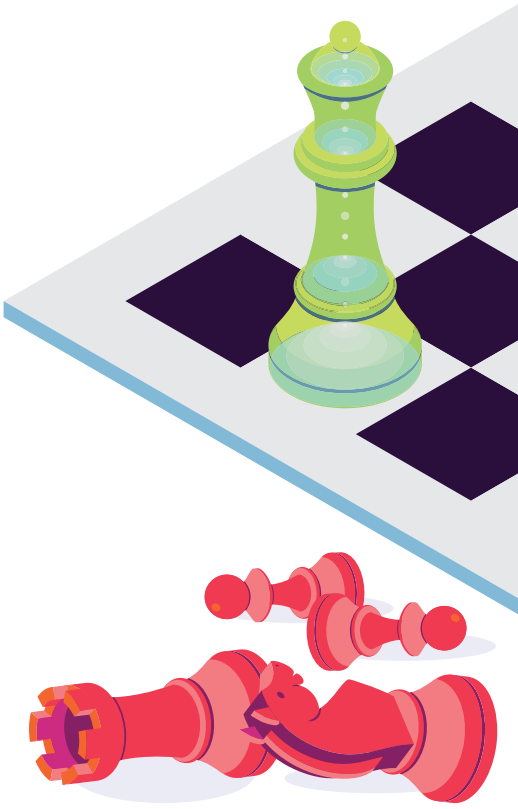
Prediction: More than one-third of executives make extensive use of AI for predicting cyber threats. The AI scans through huge amounts of data of various types to make predictions based on how the system has been trained. Preemptive actions can then be taken to avoid attacks.

The GE Digital Alliance Program – a partnership with companies for the growth of a digital industrial ecosystem – announced the onboarding of an industrial cybersecurity platform that leverages machine learning for reducing industrial internet of things (IIoT) and industrial control system (ICS) risks. The intent is to use the non-intrusive operational technology platform to automatically identify their assets and network topology, identify critical vulnerabilities, and continuously monitor their networks for any destructive cyberattacks.[10]

Response: AI is still at a relatively nascent stage when it comes to actually responding to cyber-threats. We found that less than 18% of organizations make significant use today of AI for cyber threat response. However, AI can be used to reduce the time taken to create a virtual patch for a detected threat or develop new protection mechanisms for evolving technologies. "Currently response processes tend to be very rule-based," explains Stephen Schmidt, CISO, AWS. "We will get better when the response platforms can take a generic input and produce a broader output. For example, if you see an attack proceed against one machine, then respond by blocking that attacker on all machines which are similarly situated."

Hong-Kong-based CITIC Telecom has incorporated AI-based applications into its managed security service provider (MSSP) offering. This solution builds and understands the "pattern of life" of every user and device on a network. The AI algorithms can identify threats in real time and respond autonomously – akin to using "digital antibodies" to neutralize attacks. Daniel Kwong, senior vice president, Information Technology and Security Services at CITIC Telecom CPC says, "As we have seen from the headlines, humans are consistently outpaced by increasingly automated threats, organizations increasingly recognize that traditional defenses focused on past threats only provide the most essential protection."[11]

Similarly, US-based specialty retailer Avenue uses machine learning to protect its websites and apps from bot attacks. Avenue was alerted to the problem when customers noticed fraudulent orders for merchandise placed on their accounts. An investigation by the security team revealed that attackers used bots to target the company, mounting account takeover attacks using stolen logins and passwords.[12] To combat the attacks, Avenue deployed a 'bot defender' solution. The bot defender uses machine learning to tell the difference between normal behavior and anomalous behavior, shutting down bot-triggered anomalous behavior.[13]



51%

Share of organizations that have high utilization of AI for detection of cybersecurity threats

How organizations are benefitting from AI in cybersecurity

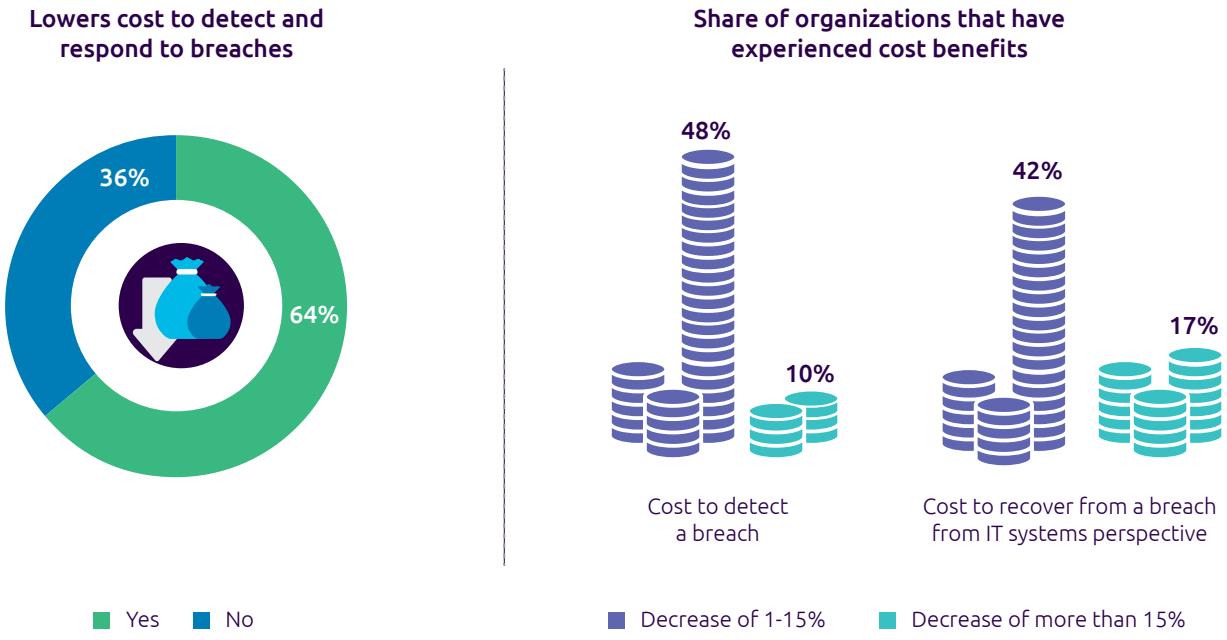
Our findings indicate those organizations that have implemented AI in cybersecurity are realizing significant benefits. Two out of three organizations say AI increases ROI on cybersecurity tools. Take global electrification, automation, and digitalization leader Siemens AG, for example. The Siemens Cyber Defense Center (CDC) used AWS (Amazon Web Services) to build an AI-enabled, high-speed, fully automated, and highly scalable platform to evaluate 60,000 potentially critical threats per second. Because of the AI, they were able to manage this capability with a team of less than a dozen people and without impacts to system performance.[14]

AI lowers the cost to detect and respond to breaches

Using AI for cybersecurity enables organizations to understand and reuse threat patterns to identify new threats. This leads to an overall reduction in time and effort to identify incidents, investigate them, and remediate threats.

Close to two-thirds of executives (64%) say that AI lowers the cost to detect and respond to breaches. The reduction in cost for a majority of organizations ranges from 1% – 15% (with an average of 12%). However, a few organizations have managed to achieve even higher cost reductions (more than 15%) leading to higher benefits (see Figure 4). "AI offers huge opportunities for cybersecurity," says Oliver Scherer, CISO of Europe's leading consumer electronics retailer, MediaMarktSaturn Retail Group. "This is because you move from detection, manual reaction and remediation towards an automated remediation, which organizations would like to achieve in the next three or five years."

Figure 4: AI in cybersecurity lowers the cost to detect and respond to breaches



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

AI makes organizations faster at responding to breaches

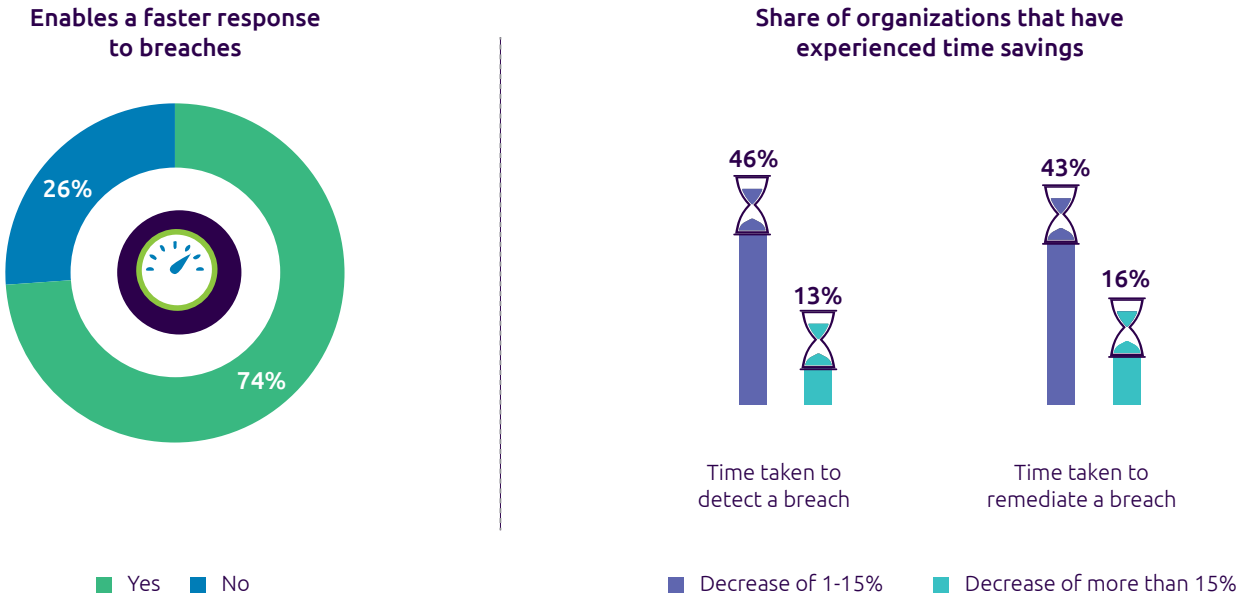
Fast response is essential to securing an organization from cyber attacks. With AI, the overall time taken to detect threats and breaches is reduced by up to 12%. AI also reduces the time taken to remediate a breach or implement patches in response to an attack by 12%. A small subset of organizations even managed to reduce these time metrics by greater than 15% (see Figure 5).

zPower, a leading rechargeable battery manufacturer, partnered with a startup to use AI to detect and autonomously respond to threats as they emerge. Just weeks after the solution was deployed, the security team was alerted to the fact that an employee had downloaded potentially malicious software. They were able to remove the threat and head off any attack in real time.[15]

Dwell time – the amount of time threat actors remain undetected – drops by 11% with the use of AI. This time reduction is achieved by continuously scanning for known or unknown anomalies that show threat patterns.

PetSmart, a US-based specialty retailer, was able to save up to $12 million by using AI in fraud detection. The company implemented an AI/ML technology that aggregates millions of transactions and their outcomes. The technology determines the legitimacy of each transaction by comparing it against all other transactions received. As fraudulent orders were identified, they were cancelled, saving the company money and avoiding damage to the brand.[16]

Figure 5: Nearly three in four executives say AI in cybersecurity enables a faster response to breaches



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

With AI, the overall time taken to detect threats and breaches is reduced by up to 12%

> **AI offers huge opportunities for cybersecurity. This is because you move from detection, manual reaction and remediation towards an automated remediation, which organizations would like to achieve in the next three or five years."**
> **Oliver Scherer,**
> **CISO, MediaMarktSaturn Retail Group.**

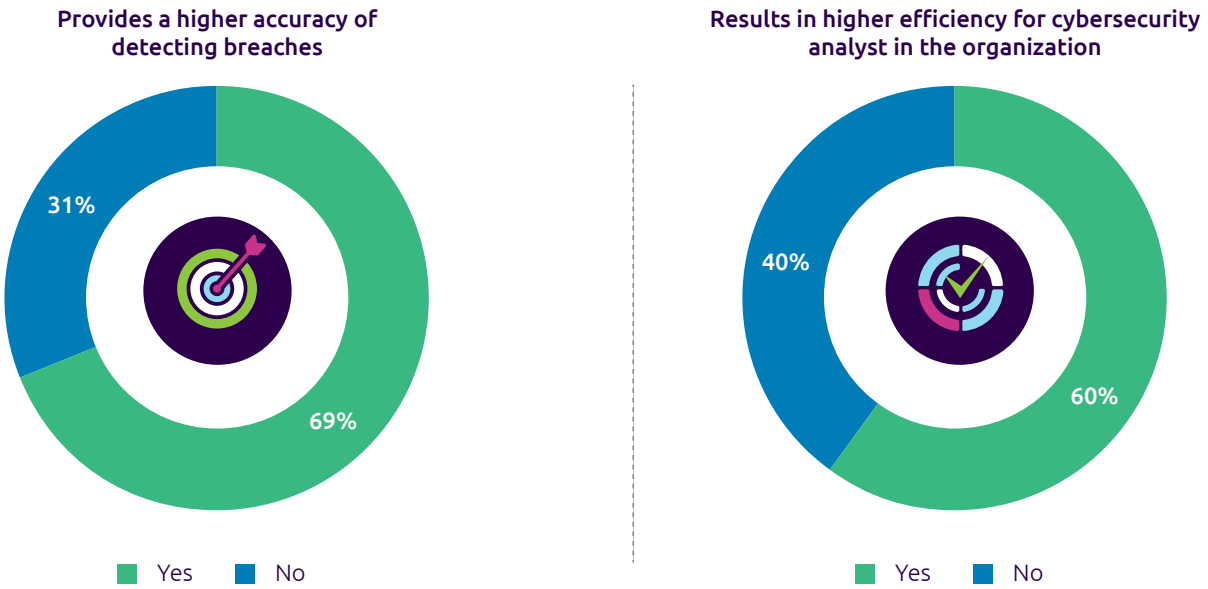
AI results in higher efficiency for cyber analysts

Cyber analysts spend considerable time going through data logs and/or incident timesheets. With AI helping carry that workload, cyber analysts can spend more quality time analyzing the incidents identified by the AI cybersecurity algorithms.

Half of organizations say that hiring for AI in cybersecurity is a high priority in their organization. However, talent is scarce in the cybersecurity field as a whole, and AI can help close the talent gap. "Cybersecurity will require a significant workforce with deep domain knowledge," says Agustin Valencia, head of OT cybersecurity for Iberdrola, a Spanish electric utility. "AI will support analysts in matching the dots, using good data to analyze the potential threat," he says.

Three in five executives agree that AI in cybersecurity improves the accuracy and efficiency of cyber analysts.

Figure 6: AI can help organizations provide a higher accuracy of detecting breaches



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

AI results in new revenue streams through cybersecurity offerings

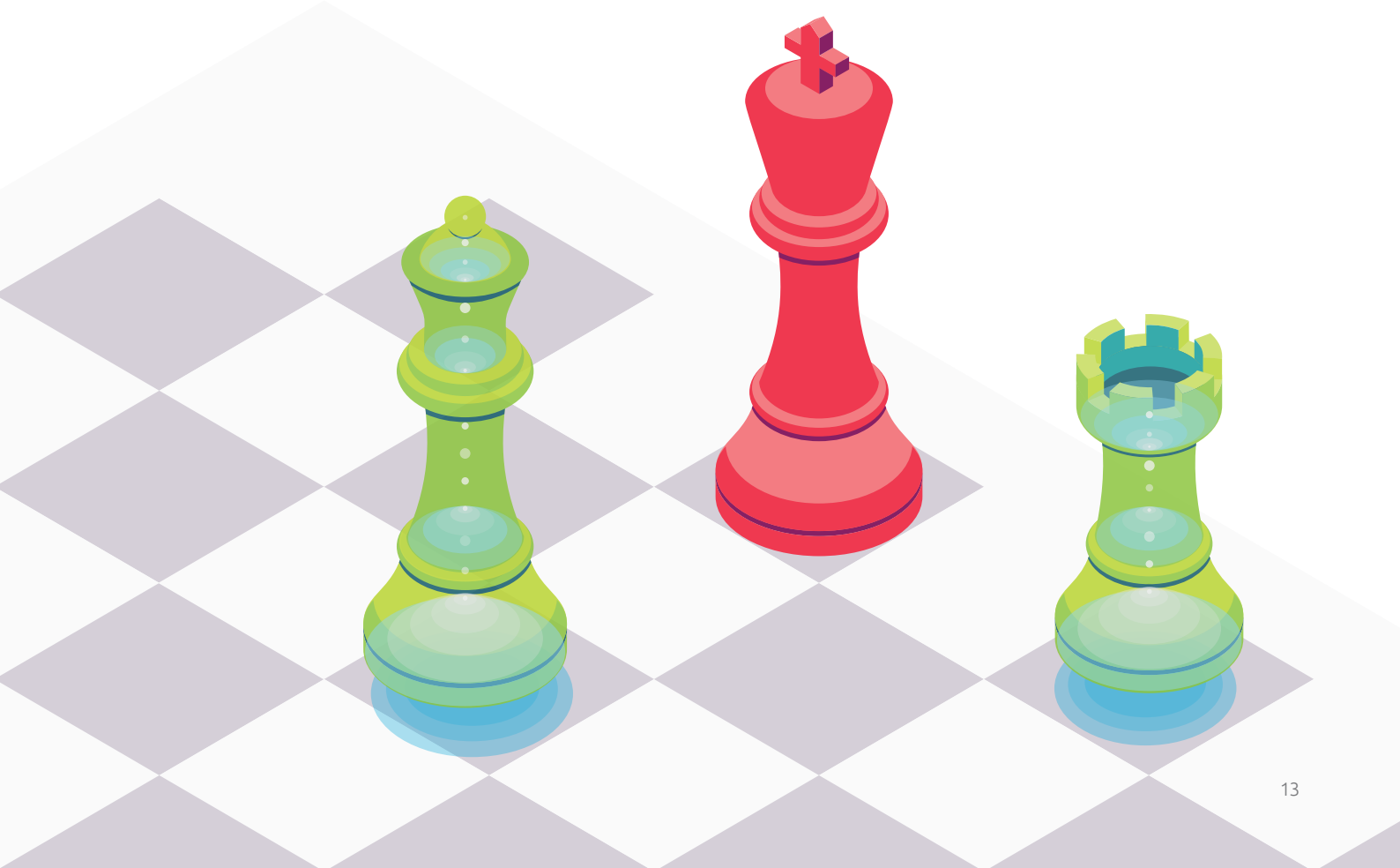
With the proliferation of smart products – electronic devices generally connected wirelessly to other devices or networks – the attack surface for hackers increases. This creates an opportunity – offering cybersecurity services to manufacturers that sell smart products. A number of organizations are already targeting this opportunity:

GE's *Digital Ghost* technology offers an AI-enabled protective layer for industrial control systems. *Digital Ghost* leverages the digital twins (which are often referred to as the brains of the associated control systems) to gain knowledge of the machine's working pattern. *Digital Ghost* detects if the machine, while appearing to operate normally, is actually being influenced by cyber attacks.[17]

Similarly, **Siemens'** *'Industry Anomaly Detection'* solution uses AI to detect anomalies, either via intrusion or data theft by hackers. The solution analyzes data traffic in the network in a learning phase to establish transparency of every device connected to the network. It can then identify any vulnerabilities while providing continuous monitoring to detect anomalies.[18]

69%

Share of executives who say AI in cybersecurity provides a higher accuracy of detecting breaches.



Where should organizations focus their AI cybersecurity initiatives?

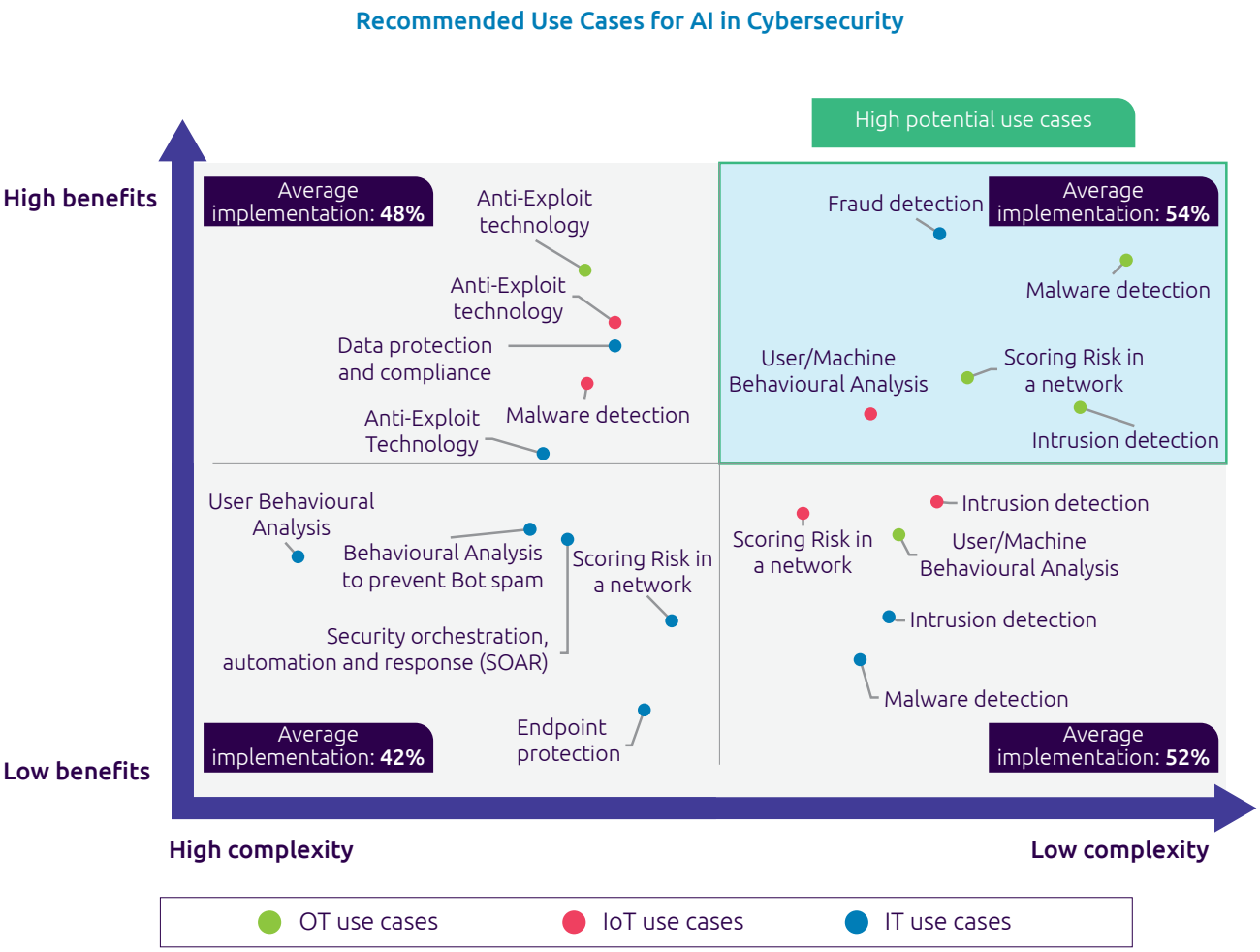
For organizations seeking to optimize value and justify further investment in AI-enabled cybersecurity solutions, identifying high-potential use cases to implement initially is key to ensuring quick wins for AI in cybersecurity. Fifty-seven percent of our surveyed executives said that a lack of understanding of high-potential use cases (those that are easy to implement and that provide benefits quickly) is an implementation challenge.

We analyzed twenty such use cases across information technology (IT), operational technology (OT) and the internet of things (IoT) and ranked them according to their implementation complexity and resultant benefits (in terms of time reduction).

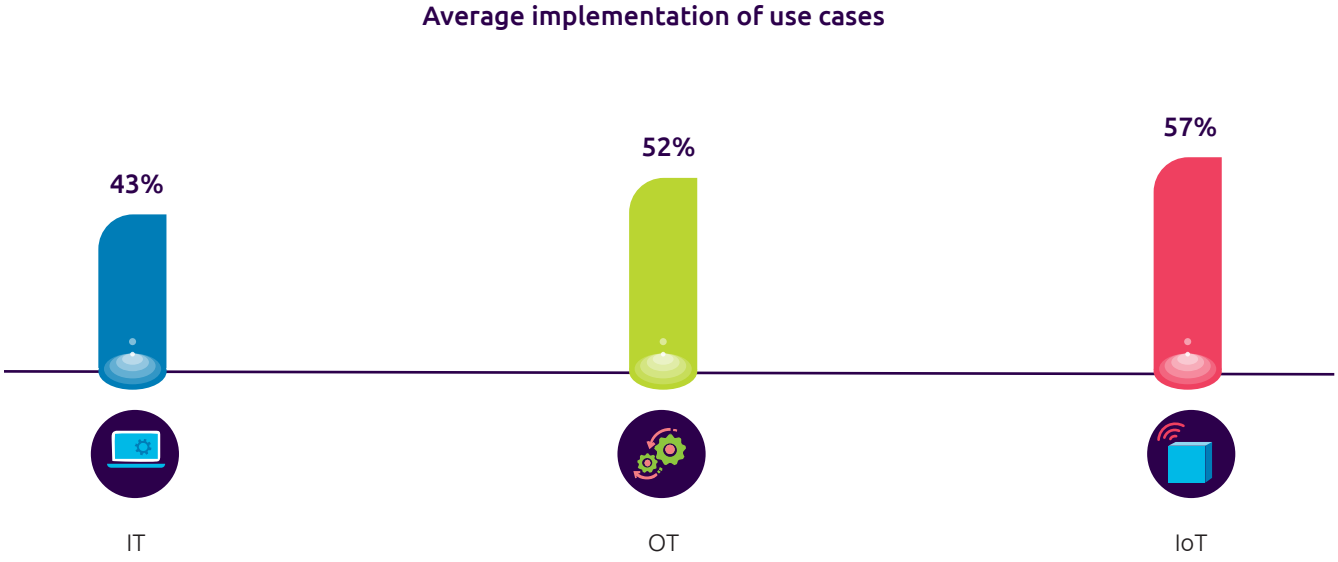
High-potential use cases for AI in cybersecurity

Based on our analysis, we recommend a short list of five high-potential use cases that have low complexity and high benefits. Overall, 54% of organizations surveyed have already implemented these high impact use cases (see Figure 7). However, another 42% of organizations admit they are implementing use cases which are highly complex and provide lower benefits. Organizations should focus on use cases that offer early benefits before tackling the more challenging use cases.

Figure 7: OT and IoT use cases have higher rates of adoption



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives
Average implementation: Share of organizations that have deployed the use cases in quadrant at first level, multiple, or full-scale deployment.



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives
Average implementation: Share of organizations that have implemented use cases in IT, OT, and IoT

List of high-potential use cases

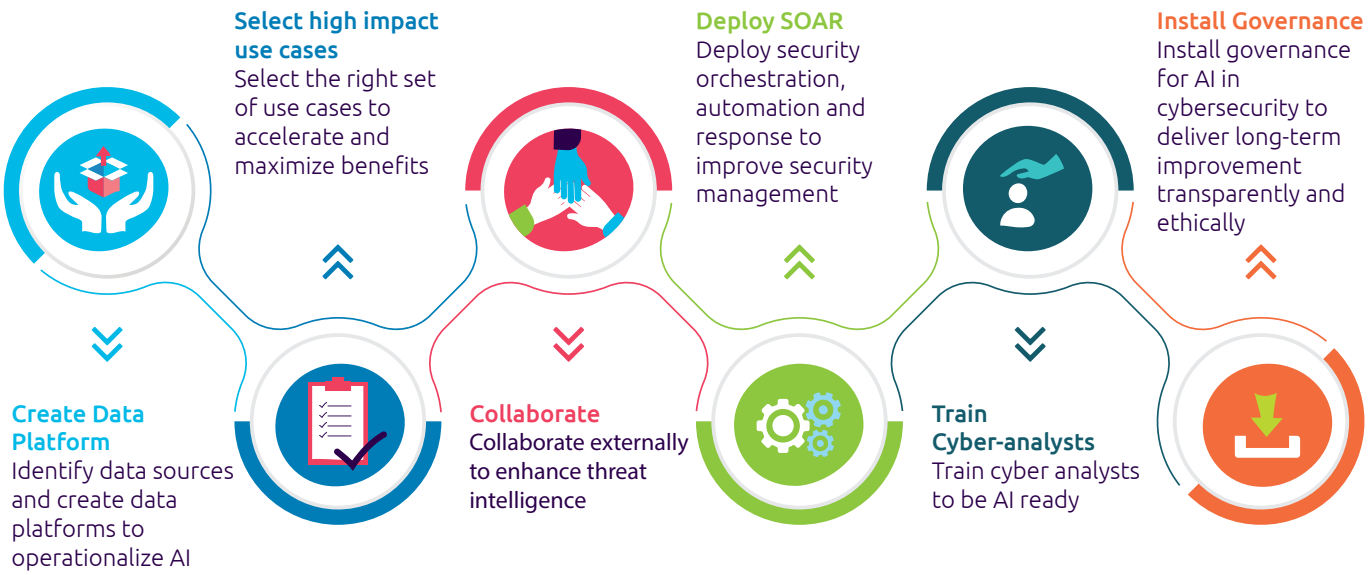
High Potential Use Case	Description	Industry Implementation
Scoring risk in the network (OT)	Compile risk ratings scores that are data-driven, quantitative, and that do not depend on domain insights from cyber analysts. The score provides estimates of scaled risk as well as data-driven uncertainty bounds, which allows faster prioritization of high-risk threats.	Verizon has AI-powered endpoint security intelligence in their Managed Security Service offering. This powers Verizon's security assessment framework to help companies identify and prioritize risks based upon varied assessment levels and to focus only on those that need immediate security action.[19]
Intrusion detection (OT)	Rapidly detect, analyze and defend against cyber attacks in real-time through automated, highly accurate insights into malicious activity.	New frameworks and research works are coming up to detect intrusions in power-distribution smart grids. For example, a team of researchers from Berkeley Labs is building up a framework that combines cybersecurity methodology, machine learning algorithms, and sensor technology into a security monitoring and analysis framework specifically for power grids to detect intrusions in the electrical grid via IP networks.[20]
User/machine behavioral analysis (IoT)	Identify behaviors that are unlikely to represent human actions. This behavior-based technology allows organizations to detect and block the most sophisticated new forms of cyber-attacks in real time with high accuracy. It also helps to improve application security by detecting compromised accounts through suspicious user behavior.	ISFM, a European autonomous shuttle company, has an AI-based behavior profiling and access control to guard the electronic control systems of its autonomous vehicles against hacking.[21]
Fraud detection (IT)	Use machine learning to detect possible fraud threats, reducing financial loss while also enhancing the user experience	PayPal managed to reduce its fraud rate to just 0.32% of revenue using a sophisticated deep learning system that analyzes transactions in real time.[22]
Malware detection (OT)	Use previously-identified characteristics of malware to predict potential future malware infections that signature-based approaches may not be able to detect.	Top players in the oil and gas industry – Duke Energy, BP, Honeywell – use AI and harness real-time sensor data from machines to intervene and avert potential problems and failures. The AI product works like the human brain to detect varied intrusions.[23]

Building a roadmap for implementing AI in cybersecurity

While the benefits offered by AI in cybersecurity are considerable, many organizations struggle to implement solutions. In our survey, we asked respondents to choose from a list of implementation challenges they faced in adopting AI in cybersecurity. The number-one ranked challenge was a lack of understanding of how to scale use cases from proof of concept to full-scale deployment. Sixty-nine percent admitted that they struggled in this area.

As with any implementation, success depends on planning. Cole Sinkford, chief information security officer at GE Renewable Energy, adds "There are so many basic things that are the building blocks of cybersecurity that you need to have in place before you start talking about really advanced things like AI." As an initial, essential step, we therefore recommend creating a comprehensive roadmap for the foundational activities required (see Figure 8).

Figure 8: Roadmap for AI in cybersecurity implementation



Source: Capgemini Research Institute analysis

Identify data sources and create data platforms to operationalize AI

AI in cybersecurity can only be successful when data sources are connected to platforms and provide inputs for AI algorithms. Half of the organizations we surveyed pointed to a significant implementation challenge: that supporting AI algorithms is difficult because of integration challenges with their current infrastructure, data systems, and applications landscapes. Although a significant majority of executives say they know what they want to achieve from AI in cybersecurity, only around half (54%) have identified the data sets required to operationalize AI algorithms.

As well as identifying the data, you also need to ensure it is up-to-date and complete if you want a high-quality output. Only half of executives say they conduct regular quality checks to ensure data sets are updated and safe to be used as input for AI algorithms. "The key challenge for implementing AI in cybersecurity is actually availability of good quality data," says DWP's Paul Owen.

Data platforms are an essential requirement to ensure a successful implementation of AI in cybersecurity. Buying or building one should be the first step for organizations.

Select the right set of use cases to accelerate and maximize benefits

To drive the benefits needed to justify the investment, selecting the right set of use cases to implement is crucial. Use case selection is a continuous process for AI in cybersecurity. With AI implementations, it takes time to run through the number of iterations required to arrive at the optimal and actionable output. Organizations should:

- Begin with the use cases that offer significant benefits, but which are also less complex to implement.
- Focus initially on use cases where the data available is complete, up to date and refreshed frequently.
- Ensure there are subject matter experts available who can verify the output from test use cases so that algorithm logic can be tweaked appropriately.

Collaborate externally to enhance threat intelligence

Collaboration with threat researchers or security professionals who are not employees through crowd-sourced platforms like Open Threat Exchange[24] is important. This helps organizations keep up to speed with the threats that other security professionals are encountering and plays an important part in improving the logic of AI algorithms to detect threats efficiently. Organizations can also create proprietary platforms to collaborate with peers to discuss and share the latest threat data. For instance, Facebook Threat Exchange[25] and IBM X-Force Exchange[26] enable organizations to share and consume threat intelligence in a convenient format. Daniel Weitzner, director of the Massachusetts Institute of Technology Policy Research Initiative, confirms ,"First and foremost, the best security teams are the ones that connected with their peers, either locally, or in their industry sector," he says.[27] Currently, only one in two surveyed executives say they share threat intelligence outside their organization through crowdsourcing platforms.

Deploy security orchestration, automation and response to improve security management

Security orchestration, automation and response (or 'SOAR')[28], are technologies that enable organizations to collect security data and alerts from different sources. SOAR allows incident analysis and triage to be performed, leveraging a combination of human and machine power. This helps define, prioritize and drive standardized incident response activities according to a standard workflow through connections to data sources and platforms. SOAR is an essential prerequisite to ensure optimal output from AI in cybersecurity, but only 36% of organizations have deployed it. The benefits from SOAR are:

- Increased alert triage quality
- Reduced time to onboard cyber analysts
- Improved security and operations center management

Train cyber analysts to be AI ready

Half of the executives surveyed said that there is a lack of qualified cybersecurity experts who are capable of improving the logic underpinning AI algorithms to detect threats efficiently. To ensure the AI algorithm can close potential threat entry points, teams need knowledge of key processes within an organization. "When analyzing attacks, you need to put together not only security experts but also process experts to understand the issues," says Iberdrola's Agustin Valencia. "AI for this case must be integrated or validated along the whole process it is trying to secure."

One way to solve this problem is to upskill employees whose roles are affected by other technology advances, such as automation, while drawing on their knowledge of the company. "What we need to do is take those people that we are removing the jobs from and train them around cyber," says Laura Barrowman, the chief technology officer at Credit Suisse. "Cyber is not just about the technical skills, it is about the knowledge of the organization. You cannot protect something if you don't know how it works."[29]

Another way to increase the efficiency of cyber analysts is to create proper interfaces for them to interact with AI tools and incident alerts. "For the short term, a good application for AI is to have intelligent chatbots that can help security operation centers to respond to high levels of demand from people needing assistance, such as when you have a ransomware dissemination," says Agustin Valencia. "We cannot have the people in the security operation center spending all their time just attending to the phone."

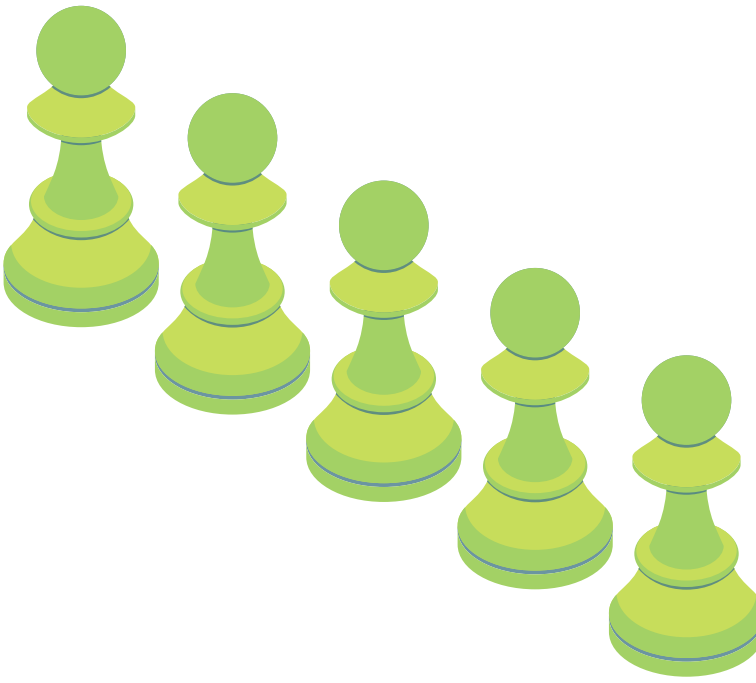
Install governance for AI in cybersecurity to deliver long-term improvement transparently and ethically

Organizations need to have a governance mechanism for their AI-enabled cybersecurity. A few tasks which must be continuously administered by the Security and Operations Center (SoC) are:

- Defining roles and responsibilities for cyber analysts
- Monitoring AI algorithm output by cyber analysts before any action is taken
- Creating control processes to monitor if an AI algorithm is behaving abnormally
- Identifying the risk tolerance for the output generated by AI algorithms
- Implementing a mechanism to monitor AI algorithms' output logic and upgrades
- Instituting a 'plan B' if AI algorithms fail or are tampered with
- Implementing key performance indicators to measure success

"The governance and the transparency around AI in cybersecurity systems are really important," says IBM's Martin Borrett. "You can't make it like a black box. It has to be tested regularly with control questions to make sure we are getting the outcomes we expect and to make sure it's performing correctly and isn't being subverted."

> **"There are so many basic things that are the building blocks of cybersecurity that you need to have in place before you start talking about really advanced things like AI."**
> **Cole Sinkford,**
> **Chief Information Security Officer,**
> **GE Renewable Energy**



Conclusion

A constantly evolving IT/OT landscape and ever-expanding attack surfaces lead to increasingly complex security challenges. Many firms have already begun exploring how AI in cybersecurity can help mitigate these risks: AI in cybersecurity adoption rates are on the rise. For firms that have yet to start using AI in cybersecurity - as well as firms that are already using it - there are a number of steps that are critical to realizing AI's cybersecurity potential. Security departments in organizations should identify where deploying AI in cybersecurity can bring the most value and then establish appropriate goals. Organizations next need to build a roadmap that addresses infrastructure, data systems, applications landscapes, skill gaps, best practices, governance, and use case selection and implementation. Taking these actions will enable organizations to avoid unnecessary losses and, in some cases, even add additional sources of revenue.

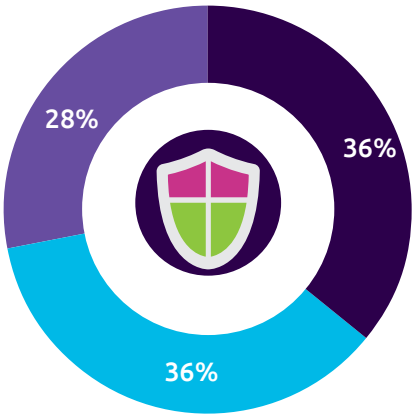
Research Methodology

Primary surveys

Executive survey:
We surveyed 850 senior executives, director level and above, spread across seven sectors: Consumer products, retail, banking, insurance, automotive, utilities, and telecom. One fifth of the executives are CIOs and one in ten are CISOs in their respective organizations.

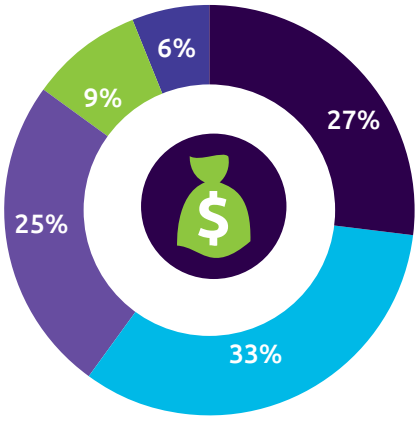
Executives belong to companies headquartered in: France, Germany, the UK, the US, Australia, the Netherlands, India, Italy, Spain, and Sweden.

By organizational unit



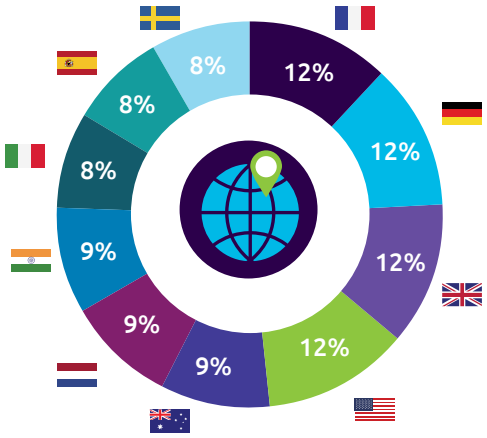
- IT Information Security
- Cybersecurity
- IT Operations

By revenue



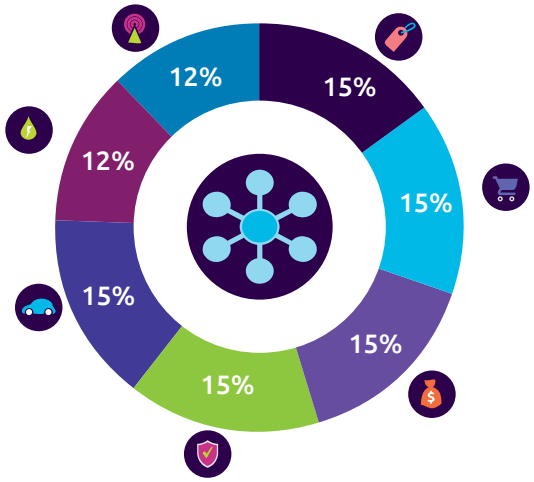
- US$1- $5 billion
- US$6-$10 billion
- US$11-$20 billion
- US$21-$50 billion
- More than US$50 billion

By country



- France
- Germany
- UK
- US
- Australia
- Netherlands
- India
- Italy
- Spain
- Sweden

By sector



- Consumer Products
- Retail
- Banking
- Insurance
- Automotive
- Utilities
- Telecom

Focus interviews:
We also conducted interviews with industry leaders and academics, examining the current status and impact of AI in cybersecurity

References

1. Cybersecurity Ventures, “2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics,” February 2019.
2. Raconteur, “AI in cybersecurity: a new tool for hackers?,” February 2019
3. Cisco, “Visual Networking Index(VNI) Forecast Highlights Tool”, December 2018
4. TheDrive, “Hacker Claims Ability to Remotely Shut Off Car Engines While Vehicles Are in Motion,” April 2019.
5. CIO, “Top 10 strategic IoT technologies and trends: Gartner,” November 2018.
6. LightReading, “AT&T’s Gilbert: AI Critical to 5G Infrastructure,” September 2018.
7. Forbes, “The Eye of Cybersecurity: How Machine Learning Sees Vulnerability,” January 2019
8. Darktrace, “Sunsweet Case study.”
9. HelpnetSecurity, “Honeywell’s industrial cybersecurity solution guards against USB device attacks,” February 2019.
10. Control Design, “CyberX partners with GE to strengthen IIoT cybersecurity,” December 2018.
11. TechCrunch, More funding for AI cybersecurity: Darktrace raises $75M at an $825M valuation,” July 2017.
12. PerimeterX, “Avenue Stores PerimeterX Case Study,” 2018.
13. Techcrunch, “PerimeterX secures $43M to protect web apps from bot attacks,” February 2019.
14. AWS, “Siemens Handles 60,000 Cyber Threats per Second Using AWS Machine Learning,” April 2019.
15. Darktrace, “Darktrace Stops Emerging Insider Threat at Battery Plant,” October 2017.
16. ZDNet, “How technology is saving PetSmart millions by eliminating sales fraud,” July 2018.
17. GE “Digital Ghost: Real-Time, Active Cyber Defense,” January 2019.
18. Siemens, “Siemens heightens industrial cyber security by detecting anomalies,” April 2018.
19. Cylance, “Verizon Expands Managed Security Services Portfolio with BlackBerry Cylance AI-Based Endpoint Security,” March 2019.
20. TechRepublic, “Power grid cybersecurity tool uses machine learning and sensors to detect threats,” March 2018.
21. Milla Group, “ISFM and SafeRide Technologies announce first technology and commercial partnership to protect autonomous shuttle from cyberattacks,” October 2018.
22. IPSwitch, “How AI Is Helping The Finance Industry Prevent Fraud,” July 2017.
23. CNBC, “SparkCognition 2017 Disruptor 50”, May 2017
24. AlienVault, “About Open Threat Exchange (OTX)”
25. Facebook, “ThreatExchange Documentation”
26. IBM, “X-Force Exchange”
27. Government technology, “MIT Cybersecurity Expert Stresses Importance of Collaboration,” March 2017
28. Gartner, “Preparing Your Security Operations for Orchestration and Automation Tools,” February 2018
29. TechRegister, “Credit Suisse tech head on automation,” Jan 2019.

Authors

Ron Tolido
Executive Vice President and CTO,
Capgemini Insights and Data
ron.tolido@capgemini.com

Ron is the lead-author of Capgemini's TechnoVision trend series and responsible for Artificial Intelligence within Capgemini's Chief Technology & Innovation Network. With global clients, he focuses on innovation, agile architecture, digital strategy and AI.

Geert van der Linden
Cybersecurity Business Lead
geert.vander.linden@capgemini.com

Geert is the cybersecurity business lead of Capgemini's Global Cybersecurity Practice. Prior to this, Geert held roles as CIO of Capgemini's Infrastructure Services Strategic Business Unit (SBU) and Security practice lead in the Cloud Infrastructure Services SBU.

Luis Delabarre
CTO, Cybersecurity
luis.delabarre@capgemni.com

Luis Delabarre is the Cybersecurity CTO for Capgemini where he helps enterprises combat cyber threats and improve their security posture. He is also a member of various security industry working groups and think tanks, leading discussions on topics such as cloud and cybersecurity. In his earlier roles, Luis was involved in very large projects in the areas of telcom, banking and transportation and also supported major accounts in defining complex architectures and deploying critical infrastructures, in particular involving virtualization, encryption and cloud.

Jeff Theisler
Managing Consultant, Capgemini Invent North America
jeffrey.theisler@capgemini.com

Jeff Theisler is a managing consultant with Capgemini Invent. He helps clients solve complex business problems, with and without the use of technology-based solutions. Recently, he has been working with the Capgemini Research Institute exploring topics of global interest.

Yashwardhan Khemka
Manager, Capgemini Research Institute
yashwardhan.khemka@capgemini.com

Yash is a manager at the Capgemini Research Institute. He likes to follow disruption fuelled by technology across sectors.

Anne-Laure Thieullent
Managing Director, Artificial Intelligence & Analytics Group Offer Leader
annelaure.thieullent@capgemini.com

Anne-Laure leads the Artificial Intelligence & Analytics Capgemini Group Offer (Perform AI), one of Capgemini's 7 Group Portfolio Priorities. She advises Capgemini clients on how they should put AI technologies to work for their organization, with trusted AI at scale services for business transformation and innovation. She has over 19 years of experience in massive data, analytics and AI systems.

Allan Frank
Vice President & CTO, Capgemini Invent – North America
allan.frank@capgemini.com

Allan is the Chief Technology Officer for Capgemini Invent in North America. He also leads the Data Solutions practice. Allan focuses on the application of transformational technologies, in particular, the disruptive role of Artificial Intelligence in the Re-Imagined Enterprise. Allan is also a recognized expert in the areas of information delivery, decision support and knowledge management.

Jerome Buvat
Global Head of Research and Head of Capgemini Research Institute
jerome.buvat@capgemini.com

Jerome is head of the Capgemini Research Institute. He works closely with industry leaders and academics to help organizations understand the nature and impact of digital disruption.

Sumit Cherian
Manager, Capgemini Research Institute
sumit.cherian@capgemini.com

Sumit is a manager at the Capgemini Research Institute. He leads research initiatives across sectors to help clients understand how digital technologies disrupt business landscape and consumer behavior.

The authors would like to especially thank Subrahmanyam KVJ, Abirami B, and Vikrant Phadatare for their contribution to the report.

The authors would also like to thank Odile Durand, Jeanne Heure, Chris Heaven, Sandeep Kumar, Shakti Shekhawat, Chris Cooper, Justin McCarthy, David Asfaha, Kay Ng, Richard Starnes, Steve Wanklin, Bobby Ngai, Samir Khare, Md Salim Zia, Vijayalakshmi K, Paul Lokuciejewski, Martin Sponar, Norbert Olbrich, Robert Engels, Francisco Javier Sucunza from Capgemini and Dr. Thierry Berthier from University of Limoges, Dr. Erik van der Kouwe from Leiden University, Dr. Long Tran-Thanh from University of Southhampton, Dr. Una-May O'Reilly, ALFA Group, MIT-CSAIL (US), and Dr. Yevgeniy Vorobeychik, Associate Professor, Computer Science and Engineering, Washington University, (US), for their contributions to the report.

About the Capgemini Research Institute

The Capgemini Research Institute is Capgemini's in-house think tank on all things digital. The Institute publishes researchon the impact of digital technologies on large traditional businesses. The team draws on the worldwide network of Capgemini experts and works closely with academic and technology partners. The Institute has dedicated research centers in India, the United Kingdom, and the United States. It was recently ranked Top 1 in the world for the quality of its research by independent analysts.
Visit us at www.capgemini.com/researchinstitute/

For more information, please contact:

Global

Geert van der Linden
geert.vander.linden@capgemini.com

China

Jeff Xu
jeff.xu@capgemini.com

DACH

Paul Lokuciejewski
paul.lokuciejewski@capgemini.com

Norbert Olbrich
norbert.olbrich@capgemini.com

France

Jeanne Heure
jeanne.heure@capgemini.com

India

Samir Khare
samir.khare@capgemini.com

Balaji Thiruvenkatachari
balaji.thiruvenkatachari@capgemini.com

Italy

Alessandro Menna
alessandro.menna@capgemini.com

Netherlands

Marijn Markus
marijn.markus@capgemini.com

Nordics

Robert Engels
robert.engels@capgemini.com

Spain

Carmen Dufur
carmen.dufur@capgemini.com

José Luis Díaz
jose-luis.diaz-rivera@capgemini.com

Sweden/Finland

Ulf Larson
ulf.larson@capgemini.com

United Kingdom

Chris Cooper
chris.cooper@capgemini.com

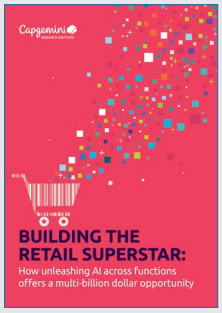
Lee Smith
lee.c.smith@capgemini.com

United States

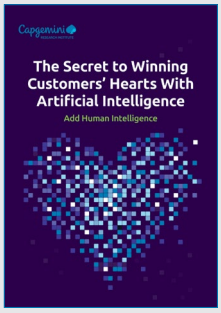
Drew Morefield
drew.morefield@capgemini.com

Discover more about our recent research on digital transformation

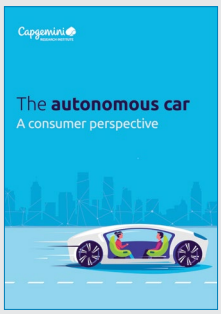
Why addressing ethical questions in AI will benefit organizations



Building the Retail Superstar
How unleashing AI across functions offers a multi-billion dollar opportunity



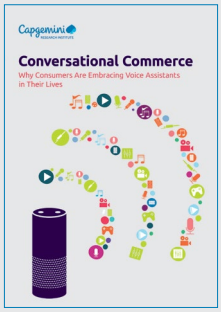
The Secret to Winning Customers' Hearts With Artificial Intelligence



The Autonomous Car
A Consumer Perspective

Digital Transformation Review 12 – Taking Digital Transformation to the Next Level: Lessons from the Leaders

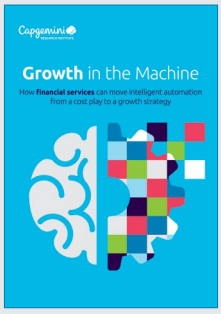
Digital Transformation Review 11 – Artificial Intelligence Decoded



Conversational Commerce: Why consumers are embracing voice assistants in their lives

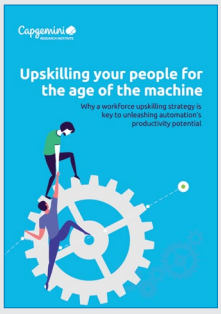
Reshaping the Future: Unlocking Automation's Untapped Value

Turning AI into concrete value: the successful implementers' toolkit



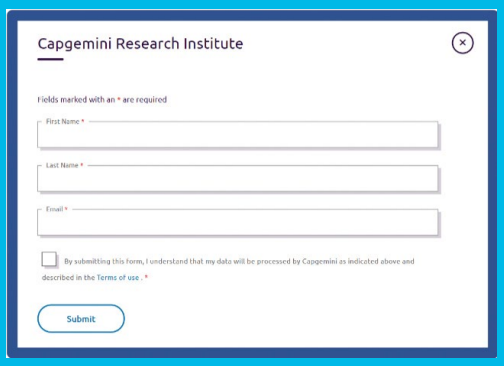
Intelligent Automation in Financial Services

Intelligent Automation in Energy and Utilities: The Next Digital Wave



Upskilling your people for the age of the machine

Subscribe to latest research from Capgemini Research Institute



Receive advance copies of our reports by scanning the QR code or visiting

https://www.capgemini.com/Research-Institute/

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

Visit us at

www.capgemini.com

MACS_CS_AP_20190508

People matter, results count.