cybersixgill

CYBERSECURITY IN 2024

Predicting the next generation of threats and strategies

Contextual threat intelligence is central to proactive cybersecurity

Over the past year, we have witnessed cybercriminal motivations evolve as they collaborate and offer their skills for hire, aiming to cause financial disruption and societal chaos. As cybercriminals aggressively employ AI, they gain more efficiency and accuracy than ever, making new types of cyber attacks a dynamic challenge that calls for proactive and adaptive cybersecurity strategies.

Today, cybersecurity is a critical business function. As cyber warfare stretches across global geographies, the surge in malicious activity has prompted increased international cooperation among governments and cybersecurity vendors to counter such threats. With the help of AI and other advanced technologies, cyber defenders are getting better at their craft.

We now face more sophisticated tactics powered by sophisticated technologies, broader targets, and higher stakes. To stay ahead of cyber attackers, companies must shift from reactive to proactive cybersecurity measures. Central to these efforts is the need for both external and internal cyber threat intelligence that is relevant and contextual to each organization, considering factors like a company's attack surface and the effectiveness of its security stack. Such a proactive approach also works in organizations' favor as they strive to maintain compliance with changing regulatory pressures - an area where contextual threat intelligence also offers significant value.

In the cybersecurity realm, predicting what will happen from one day to the next is impossible. Using comprehensive, contextual threat intelligence powered by advanced AI capabilities, we can identify the trends likely to impact organizations in the coming year. Cybercriminals will inevitably find ways to work better, faster, and smarter. Yet, cyber defenders do as well. As the cat-and-mouse game of cyberwarfare marches on, we hope Cybersixgill's insights and predictions for 2024 give you what you need to keep your assets and stakeholders safe.

Warm Regards,

Sharon Wagner
CEO, Cybersixgill

The Growth of AI

PREDICTION 01

AI will evolve to become more broadly accessible while cybersecurity vendors continue to address the reliability, diversity, and privacy of data.

PREDICTION 01

Since the launch of ChatGPT in November 2022, the primary topic of conversation in cybersecurity has been AI. With the focus on AI tools and the introduction of enterprise versions, the use of these solutions will see a significant increase in 2024.

The inherent value of AI revolves around the breadth and reliability of data, which Cybersixgill predicts will significantly improve in 2024. AI vendors will work to advance both the richness and the fidelity of results by developing the model's core technology and expanding the types of data on which AI models are trained. AI models will become highly sophisticated and able to handle diverse, hard-to-decipher data sets, such as those found on the dark web and within "hidden" data forms.

As vendors continue to break new ground with AI, security teams will feel more confident in its ability to augment security workflows with cyber threat intelligence (CTI) data. Concurrently, AI will become broadly accessible to practitioners, regardless of their skillset or maturity level. Junior-level staff will more readily rely on AI solutions to manage and take action as its value and ease of use improve. It's too soon to know if AI will close the behemoth skills gap, which today amounts to 3.5 million unfilled jobs, however, the efficiencies gained continue to grow at pace, enabling teams to deliver greater value to their organization and accelerate risk mitigation processes.

The data privacy debate

As AI's popularity expands, data privacy concerns will grow among end-user organizations, vendors, and government agencies. Government regulation of AI is still developing, as it does with most new technology innovations. In 2024, we believe many companies will form their own policies and restrictions while waiting for government entities to enact regulatory legislation. Under growing pressure, the U.S. and other countries may establish some regulation in 2024, although clear policies may not take shape until 2025 or later.

PREDICTION 01

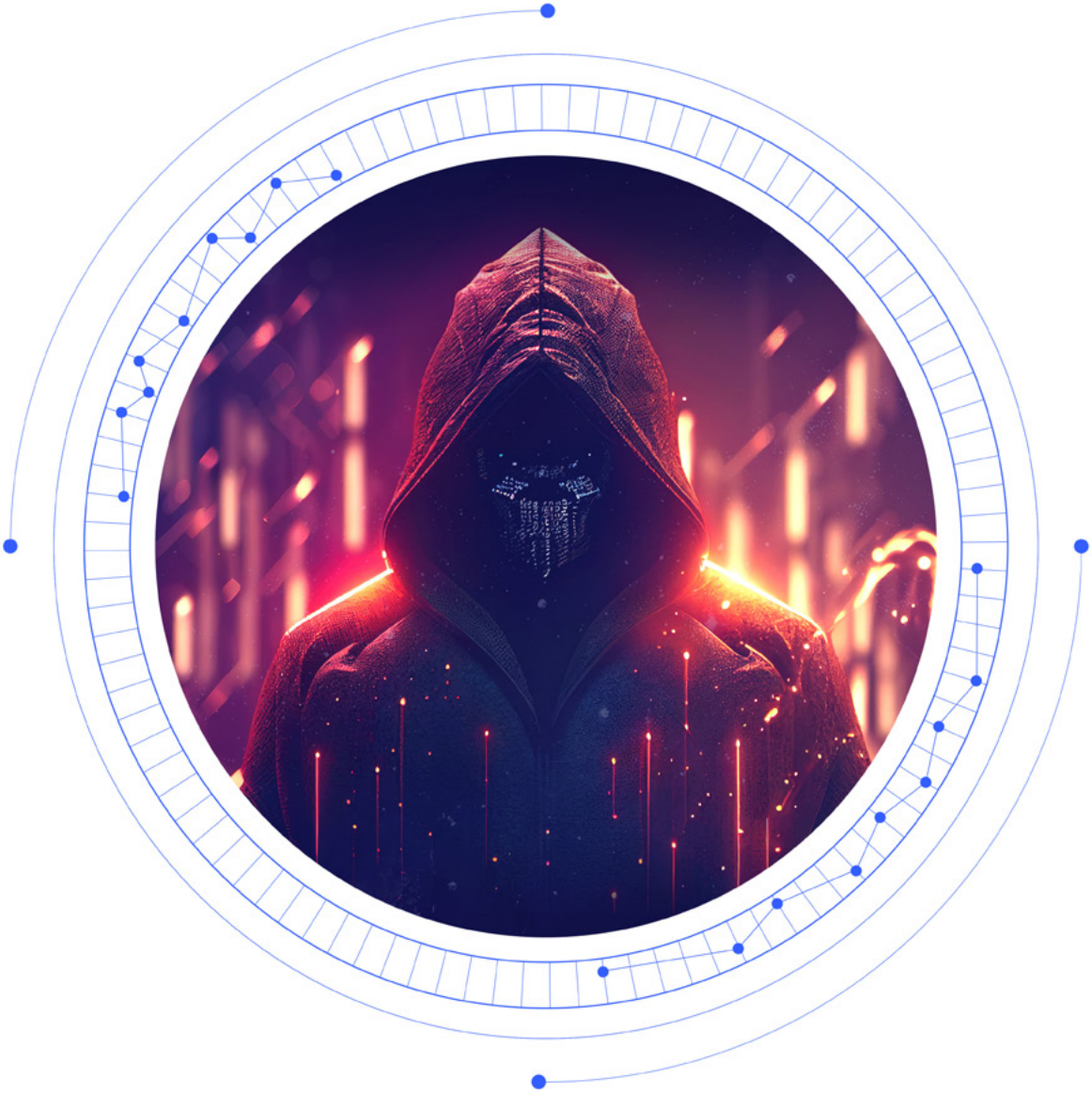
Cybersixgill is pioneering data privacy in generative AI:

Given the wealth of data available, CTI and generative AI work well together. Contextual CTI delivers important insights that help guide cybersecurity investments and approaches. When this is combined with generative AI, CISOs and their teams can access these insights quickly, regardless of skillset or maturity level. Still, data privacy concerns abound. Since the June 2023 launch of Cybersixgill IQ, our generative AI threat intelligence tool, Cybersixgill has taken the lead in protecting our customers' data. Our approach, outlined below, can provide a framework for other companies to follow.

Our approach

- **Minimize Data Transfer** to ensure that only the most essential, non-sensitive information is shared.
- **Mask Sensitive Data** to preserve the data structure for analysis while securing sensitive information.
- **Send Metadata Only** to exclude the actual content while sharing pertinent details about it.
- **Use of Differential Privacy** to publicly share information about a dataset through descriptions of group patterns while withholding and protecting individual-specific information.
- **Local Processing** in different continents to limit the data transferred over the public internet.
- **Develop Proprietary Machine Learning Models** trained locally on our sensitive data on our secure servers to ensure that we maintain control of the data and insights.

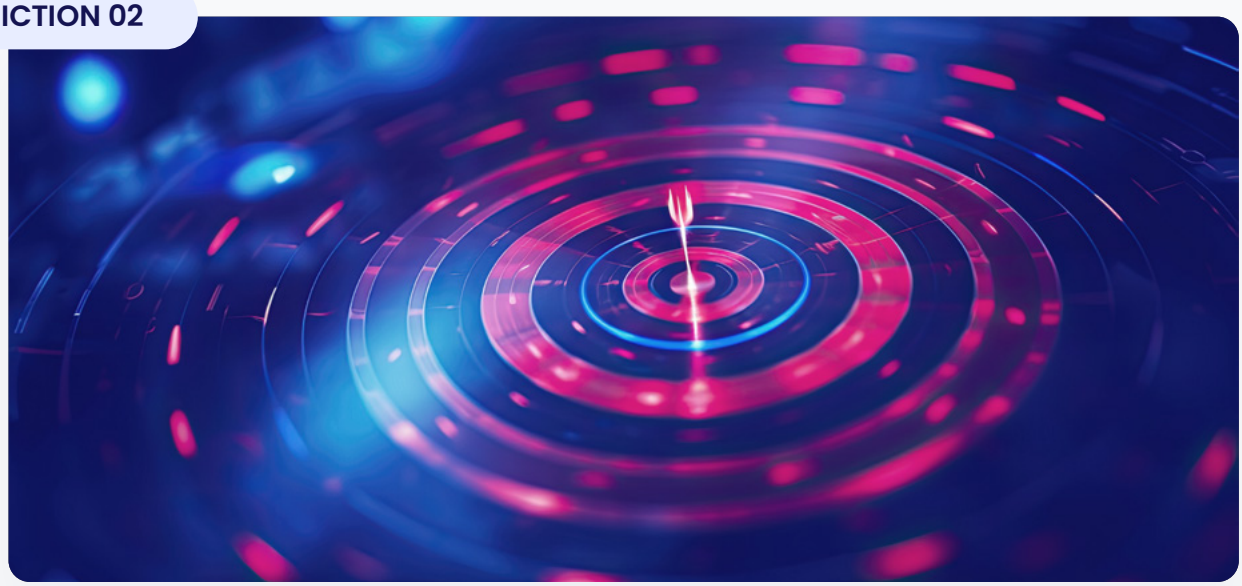
AI Attack Vectors



PREDICTION 02

AI will be used as an attack tool – and a target. Black hat hackers will increasingly use AI to improve effectiveness and the legitimate use of AI will surface as a prominent attack vector.

PREDICTION 02



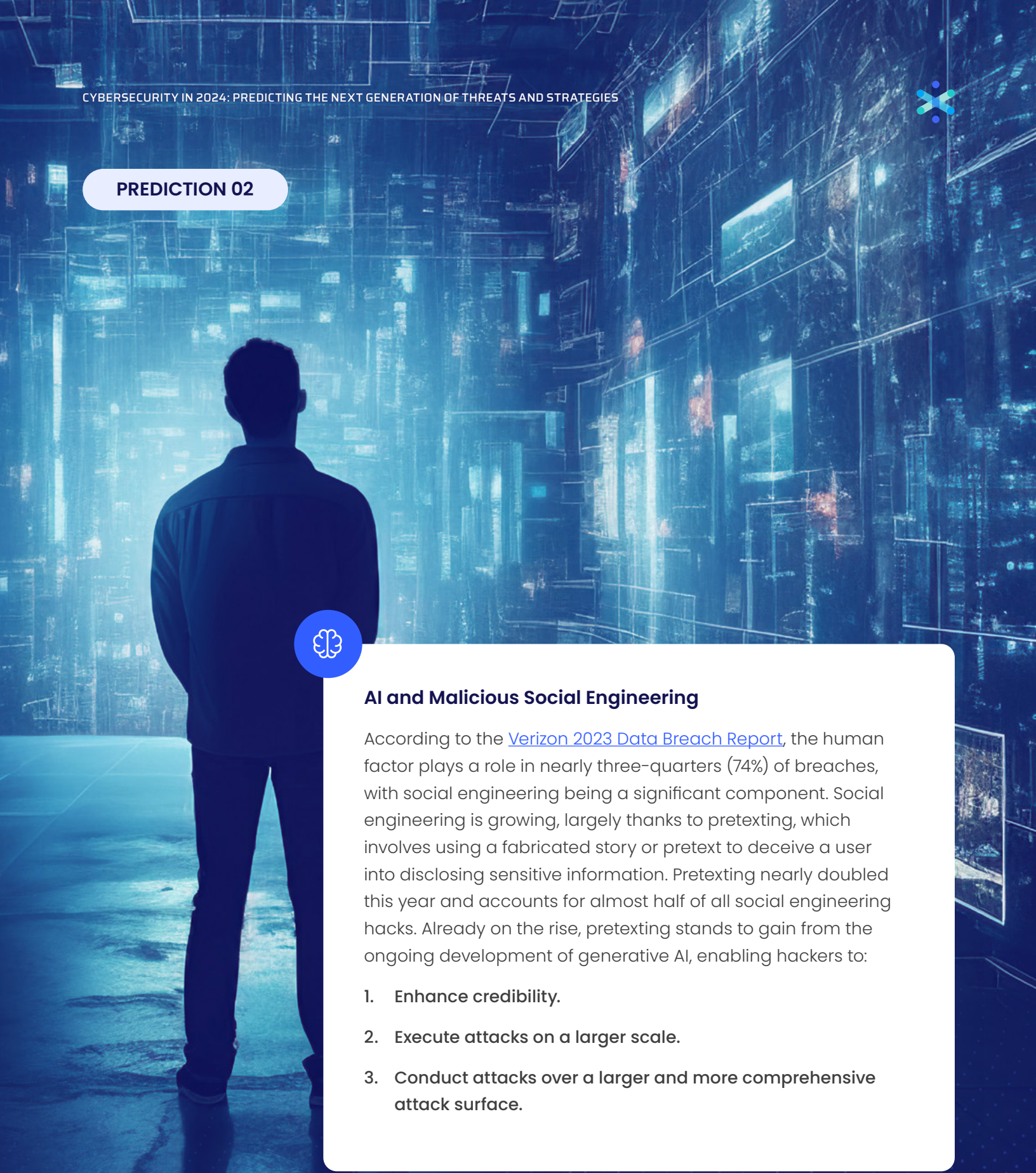
Soon after generative AI solutions were launched, it became clear that it was also a launch pad for adversarial use of the technology.

In 2024, we'll see threat actors using AI to expand the scope of their harmful activities with increasing frequency, and accuracy. Hackers will use generative AI to automate large-scale cyberattacks, create even more duplicitous, human-like phishing email campaigns, and develop malicious content that targets companies, employees, and customers across industries. .

Our research also indicates that cyber attackers will look to AI as a target through which users' credentials can be compromised and sold in underground markets. Additionally, malicious attacks like data poisoning and vulnerability exploitation in AI models will gain momentum. Data poisoning injects tampered data to control the behavior and outcome of trained AI or machine learning (ML) models and deliver false results. This could cause an organization to unwittingly provide sensitive information to untrustworthy parties or allow a threat actor to infiltrate the corporate network without detection. Similarly, AI models can be trained to identify and exploit vulnerabilities in computer networks without detection.

Adding to the list of concerns is the rise of shadow generative AI, where employees use or develop AI tools without organizational approval or oversight. Shadow generative AI can lead to data leaks, compromised accounts, and widening vulnerability gaps in a company's attack surface.

PREDICTION 02



AI and Malicious Social Engineering

According to the Verizon 2023 Data Breach Report, the human factor plays a role in nearly three-quarters (74%) of breaches, with social engineering being a significant component. Social engineering is growing, largely thanks to pretexting, which involves using a fabricated story or pretext to deceive a user into disclosing sensitive information. Pretexting nearly doubled this year and accounts for almost half of all social engineering hacks. Already on the rise, pretexting stands to gain from the ongoing development of generative AI, enabling hackers to:

1. **Enhance credibility.**
2. **Execute attacks on a larger scale.**
3. **Conduct attacks over a larger and more comprehensive attack surface.**

Compliance & Regulation

PREDICTION 03

Tighter regulations and cybersecurity mandates hold the C-suite and Boards accountable for corporations' cyber hygiene. Companies must prove vulnerability prioritization and risk management with evidence-based data.

PREDICTION 03

Government and industry regulation of companies' cybersecurity initiatives and risk posture has been evolving and tightening for several years.

For example, in 2023, the SEC introduced new rules that, among other things, make corporate executives and boards of directors more directly accountable for the protection and security of corporate and customer data and assets.

In 2024 and beyond, compulsory regulatory mandates will continue to pressure business leaders to apply enforceable rigor on security controls in response to widening attack surfaces and the growing frequency and scale of attacks. This is especially true with the increasing use of AI and the associated data privacy issues. C-suite and other executives across an organization will need a clearer understanding of their organization's cybersecurity policies, processes, and tools. Companies will increasingly appoint cybersecurity experts on the Board to fulfill progressively stringent reporting requirements and conduct good cyber governance.

According to the SEC's latest reporting requirements, companies must provide evidence-based data proving their security tools are working, gaps and vulnerabilities are adequately addressed, and events are detected and responded to effectively. Companies must now also report a cyber incident within four days of the occurrence, which continues the industry trend of shortening the window businesses have to identify and report on an incident. Additionally, changes introduced within the Payment Card Industry's Data Security Standard (PCI DSS) v. 4.0 will put added pressure on retail, healthcare, and finance companies, which will scramble to follow the new reporting requirement that must be addressed by March 2024. These changes drive a significant need for proactive threat intelligence to help mitigate risk, continuously identify gaps, and strengthen cyber hygiene.

PREDICTION 03

NIST CSF 2.0: Helping Companies Manage Cyber Risk

In 2024, a major update to the NIST Cybersecurity Framework (CSF) – NIST CSF 2.0 – is expected to be released to help organizations and industries manage cybersecurity risk. An important change in CSF 2.0 is the addition of and emphasis on governance in managing risk. CSF 2.0 includes additional updates, such as:

- **A focus on supply chain risk management**
- **More guidance on implementing the CSF**
- **Alignment with the Biden Administration's National Cybersecurity Strategy**

NIST CSF 2.0 is helping push the industry toward proactive prioritization and risk-ranking gap analysis to enable an accurate measure of system risk. Proactive risk prioritization based on comprehensive, contextual, and historical threat intelligence coupled with active control over the enterprise can alleviate many of the compliance headaches CISOs face.

To achieve this, security teams can take the following steps:

1. Define the company's governance process to understand and disclose the interrelation between cybersecurity policy, business-as-usual activities, and various stakeholders. As companies develop more security processes and risk management policies, they have a greater need for asset-aligned contextual CTI that reveals and defines how data and the enterprise stack are protected.
2. Conduct a thorough risk assessment that weighs risks both within the organization and across the supply chain against the effectiveness of core security controls that protect data.
3. Quantify cyber risks through a comprehensive CTI solution that identifies and enriches measurement of an enterprise's vulnerabilities and helps entities safely prioritize which gaps to address.
4. Define and measure a security awareness policy to determine if employees, business partners, third-party suppliers, and others fully understand and follow such policies.

Proactive Cybersecurity

PREDICTION 04

The need for proactive cybersecurity combined with continued tool consolidation will underscore the necessity of cyber threat intelligence in critical business decision-making.

PREDICTION 04

In recent years, there has been much talk and little action in using CTI's data and insights to inform critical business and operational decisions – but this is changing.

The emergence of new attack vectors and a continual increase in the frequency, scale, and cost of a breach are driving the adoption of Threat Exposure Management (TEM), a holistic program and proactive approach to cybersecurity. CTI is a foundational component of any TEM program. As such, companies will need robust CTI solutions that will deliver focused insights to initiate actions that significantly mitigate business and operational risk.

As part of the larger cybersecurity consolidation trend in recent years, Cybersixgill predicts that in 2024, the consolidation of CTI will also gain prominence as it combines with other capabilities, including attack surface management and digital risk protection. Ultimately, more companies will leverage consolidated CTI solutions that deliver essential business context, reducing the overwhelming volume of "noise."

Particularly when enhanced with AI, this type of contextual CTI empowers organizations to deploy strategic, operational, and tactical threat intelligence for use across the organization to minimize the mean time to detect and counter threats, protect assets and drive smarter cybersecurity spending. CTI will once again be viewed as a strategic enabler and organizations will begin to assess the true benefits offered by incumbent vendors, updating their provider accordingly.

PREDICTION 04

Threat Exposure Management: CTI as a strategic encore

The march towards TEM underscores the strategic value of CTI, as businesses need the data and insights it provides to feed all TEM components.

Gartner's definition of TEM comprises of five main elements:

- Scoping the organization's attack surface for vulnerable entry points and assets
- Discovering assets and their risk profiles, including visible and hidden assets, vulnerabilities, misconfigurations, and other risks.
- Prioritizing the organization's high-value assets with a plan of treatment to address them.
- Validating how attacks might work and how systems might react based on the treatment plan in step 3.
- Mobilizing people and processes and ensuring the TEM plan is communicated well and understood clearly by the security team and business stakeholders.

Geopolitical Threats

PREDICTION 05

Geopolitical and other issues will broaden attackers' motivations beyond financial gain, resulting in a growing pool of targets, attack vectors and tactics.

PREDICTION 05

Cybercriminals will continue to benefit from a widening digital landscape and new attack vectors as companies further digitize operations, expand reliance on IoT and other network-connected devices, and collect and store more data in the cloud.

For the past year or more, heightened geopolitical issues and divisive societal concerns have fed cybercriminals' motivations in new ways.

They seek notoriety by causing chaos within institutions, governments, and our everyday lives. In 2024, 40 national elections will be taking place around the world, and political leaders will be vying for supremacy. Voters in these countries represent an estimated 41% of the world's population and 42% of its GDP - the potential opportunity to disrupt proceedings will ultimately prove too tempting.

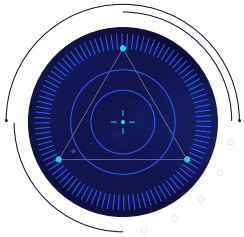
While threat actors will likely always yearn to achieve monetary gain (while wreaking financial havoc on individuals and corporations), we predict that in 2024, we'll see an uptick in attacks targeting entities previously secondary to more lucrative targets. Schools, hospitals, public utilities, and other essential services will all be considered fair game, as bad actors aim to gain power and influence and cause general disorder in the world.

To keep up with the growing minefield of opportunities and feed their expanding motivations, in 2024, we believe that cybercriminals will increasingly offer their skills and expertise for hire. Specifically, ransomware-as-a-service, malware-as-a-service, and DDoS-as-a-service offerings that target individuals, businesses, and critical infrastructure will gain in popularity. By purchasing the services, infrastructures, or tools of highly sophisticated hackers, threat actors can outsource the groundwork required to launch a successful cyber attack with very little effort.

Affiliate programs will continue to grow as powerful cybercriminal gangs franchise their ransomware technology, scaling operations to a network of lesser-skilled individuals for distribution and making the extortion business accessible and profitable to a larger pool of threat actors.

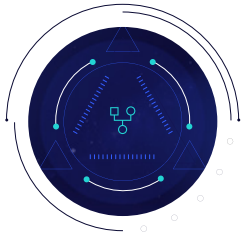
Conclusion

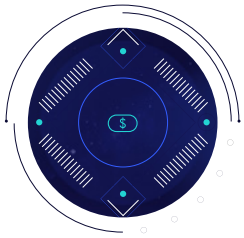
There is one certainty in cybersecurity – there will be more breaches, and the costs will continue to climb. We are at the cusp of multiple societal, economic, and technological innovations changing life as we know it, further blending our physical and digital lives.



The task of anticipating future technology needs while safeguarding existing infrastructure and assets to minimize risks and seize new opportunities is a complex and difficult one. Any approach to cybersecurity must be in lock-step with an organization's business goals, but achieving such harmony is often derailed by numerous external forces. Market disruption—fueled by technological change, complex global regulations, geopolitical tensions, and economic uncertainties—will test organizations' approach to risk and resilience.

We believe our predictions for 2024 will contribute to the next wave of business transformation, combining AI, machine learning, and other digital innovations to enable greater efficiencies and compelling customer experiences. As the stakes reach new heights, so must businesses' approach to cybersecurity – a movement well underway that will continue in the coming year.





About Cybersixgill

Cybersixgill continuously collects and exposes the earliest indications of risk by threat actors moments after they surface on the clear, deep, and dark web. Our vast intelligence data lake, derived from millions of underground sources, is processed, correlated, and enriched using automation and advanced AI. Cybersixgill captures, processes and alerts teams to emerging threats, TTPs, IOCs and their exposure to risk based on each organization's complete attack surface and internal context.

Our extensive body of threat intelligence data can be consumed through various solution offerings and integrations, each addressing critical customer pain points and use cases. These solutions are scalable, searchable and seamlessly integrated into existing security stacks, quickly arming enterprises, government and MSSPs alike with accurate, relevant and actionable insights to proactively block threats before they materialize into attacks.

Learn more at www.cybersixgill.com

Follow us

cybersixgill