Teneo | TAG CYBER

Teneo Cyber Insights: A New Series for CEOs

Teneo Insights / March 2023

Thus far in 2023, the security community has seen cyber attackers leverage more advanced tactics and technologies to identify vulnerabilities and compromise cybersecurity. In addition, advancements in artificial intelligence, increased disinformation and deepfakes, on-going geopolitical risks and imminent regulations contribute to an increasingly complex cybersecurity challenge for executives.

Considering these trends, many prior cybersecurity solutions touted as 'leading edge' for risk management are quickly exhibiting a shelf life, making it harder and harder for CEOs and cybersecurity executives to deliver on their near and long-term strategies. Furthermore, corporate stakeholders are demanding increased ownership and accountability for cybersecurity directly from the CEO.

With these challenges as a backdrop, my colleague Ed Amoroso and I have developed a new monthly series called 'Cyber Insights' which aims to provide CEOs with timely and actionable insights into the most contemporary and critical cybersecurity issues shaping the business world today. Our goal is to offer practical guidance that can help drive results quickly.

How Should Executives Manage AI Risk?

Artificial intelligence (AI) has recently emerged as a major innovation that can be leveraged by businesses for productivity and revenue gains. The ChatGPT prototype, for example, rose to one million users this year, faster than any other technology in history. Google, Microsoft and others are now driving the use of AI for search, browsing and other activities that have implications for every business.

Despite all the recent attention on AI, including the use of ChatGPT to write student compositions, compose storyline scripts and provide an alternate means for search, few observers have paid much attention to the cybersecurity implications of such innovation. As with any new technology, exciting advances tend to be balanced by risk concerns and AI certainly falls into this category.

In this article, we examine specifically how executives should view the cybersecurity risk implications of AI for their businesses. Our goal is to provide strategic assistance to C-Suite executives, including leaders like Chief Executive Officers, Chief Information Officers and Chief Digital Officers, who are now rallying their teams to identify the best opportunities to integrate AI into their businesses.

As we will show below, establishing an understanding of the cyber risk implications of AI is a more subtle task than just identifying the many new attacks AI can enable. Executives will instead need to follow a more mature progression toward the best AI-related decisions for their business. Our discussion is intended to help with this process.

How Organizations Assess the Cyber Risk of New Technologies

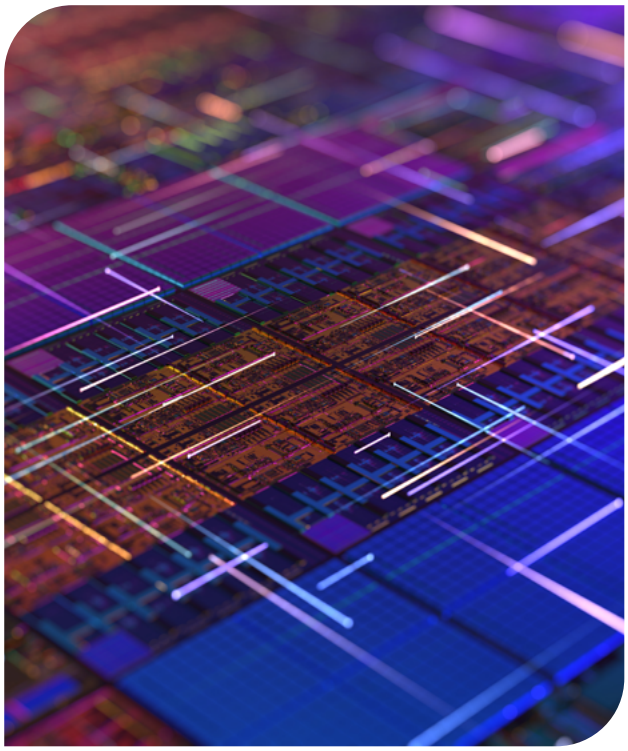
Although cyber risk has certainly gained some familiarity in the C-suite and boardroom, it helps to level-set how the best organizations assess their cyber risk posture. Two factors influence cyber risk – the potentially disruptive effects of an attack on the business (whether financial, operational, reputational) and the likelihood that such an attack might even occur.

These two factors are determined through the analysis of use-cases and are often quantified using commercial platforms. Estimates are made of attack consequences, usually in high, medium and low designations, and then comparable estimates are made of how likely it would be for such an attack to occur. The vulnerable spots for such exploitation are referred to collectively as an attack surface.

When the results of this type of risk analysis are presented to executives by the Chief Information Security Officer (CISO), a comparison is typically made against a previously established corporate decision known informally as a risk appetite. From this comparison, decisions can be made about how to reduce risk, while also driving business value with the least bit of cost and disruption.

How is Cyber Risk Determined for New Technology?

Whether doing a back-of-the-envelope review or a formal assessment with an internal or external auditor, measuring aggregate cyber risk for new technology such as AI demands two tasks. First, it must be determined whether the use



of that technology creates new security risks. For example, when AI is deployed, it is entirely possible that this could provide an adversary with a new attack target.

Second, it must also be determined if the technology itself can be used to improve the cybersecurity profile of the organization. Despite any new risks introduced, it is important to determine whether the new technology changes the nature of the attack surface for the organization. For AI, this means establishing if it can in fact be used to improve an organization's security posture.

The resulting aggregate cyber risk estimate thus demands attention to both increases and decreases that might occur. If a business call center, for example, deploys AI to help with customer inquiries, then it will see its attack surface expand through use of the new AI software. It might also, however, see a corresponding decrease in cyber risk by making its employees less prone to phishing attacks.

Executives are thus advised to demand the full story when it comes to the cyber risk estimates for new technologies such as AI. Such mature attention has allowed businesses to find ways to securely leverage tools such as Internet browsers, mobile devices and search engines that were initially thought to be much too vulnerable to threats.

How Does AI Introduce New Cyber Risks?

As suggested above, increased cyber risk from a new technology will emerge either because the attack surface has increased, thus driving up the likelihood that a breach or disruption can occur, or because the consequences of an attack have increased. Either or both cases can influence cyber risk and for AI, many different possibilities emerge.

The most common case that executives should prepare for involves AI software adding a new attack target for malicious adversaries. Whether used through human interfaces, such as ChatGPT, or automated communication, such as with an autonomous vehicle, attackers might find ways to interrupt, corrupt or bias such AI-based interactions.

The best way to address this increased probability of attack is through deployment of controls that can effectively prevent, detect or respond to exploits. Many new start-ups are emerging that provide such capability and the corporate CISO should be expected to maintain familiarity with these new offerings. AI security controls will be a growing segment of the commercial security industry.

Executives should additionally review the common case in which deployment of AI software will increase the consequences of an attack. This is best assessed through use-case analysis, often with a cyber risk quantification tool (which the CISO should be familiar with). Common sense reviews by executives will help to ensure that good decisions are being made regarding AI deployment.

A simple example is that the use of AI software to control the safety systems in a nuclear power plant could have massive consequences if the software was somehow attacked and those systems were compromised. In contrast, deployment of AI software to help HR professionals generate job descriptions certainly has consequences if compromised by a threat actor, but would have a significantly lower implication for risk and clearly no life-or-death effects.

Insight for CEOs

If deployment of AI is being considered, executives should demand to understand the impact of attack likelihood as well as the potential consequences of using AI. This is best done in the context of a previously determined risk appetite for the organization.

How Can AI Enable Improved Security?

Just as the use of AI in business can increase cyber risk, it is also entirely possible that such new technology can be used to reduce cyber risk through improvement in some procedure, process or automated system. Such attention to the potential benefits of AI for cybersecurity are often missed, especially by mainstream media or observers who only see the negative effects.

Consider, for example, how AI fundamentally reduces dependence on human actions. While this produces considerable societal concern and debate in many different contexts such as AI-generated art or music, the implications for business can be positive, especially in cases where the human being is considered a major security vulnerability.

One example is email, where for many years businesses have struggled with the problem of people inadvertently clicking on phishing links. The cyber implications have been enormous, with many ransomware outages starting with precisely this human error. As one might expect, AI software will likely soon reduce this risk by augmenting or changing how businesses handle and manage email.

For example, AI-managed robotic assistants could certainly emerge that will train on a user's normal email patterns. Once the learning process is sufficiently mature, the assistant could easily begin to manage an email in-box, thus freeing the individual for other tasks. More importantly, such deployment of AI-assisted email usage would reduce or even remove phishing risk.

Similarly, consider that humans are vulnerable to social engineering attacks, often done through human-to-human voice or chat interactions. Help desks, for example, involve people helping people, and while this has been the model for decades, AI software might prompt new use-cases. One could reasonably expect that the AI software would be much less vulnerable to tricks by adversaries.

Insight for CEOs

If deployment of AI is being considered, then executives should seek to understand if this can be used in a manner that reduces the consequences of an attack by changing the nature of how the business operates, including its dependence on error-prone human action.

Conclusion

The cyber risk implications of AI for business, as suggested above, will likely include both positive and negative impacts. The advantage of taking into consideration the full cyber risk equation is that a much clearer picture will emerge for how AI will impact the organization. As we noted, CEOs and their leadership teams are actively inventorying opportunities to transform their organizations using AI. Paramount to those discussions is a keen examination of and consideration for the interplay between strategic deployment of AI and risk management. Without such mature examination, certainly in the context of the local risk appetite, companies might opt to avoid use of AI and thus miss out on the many advantages it can produce for both revenue growth and cost improvement.

Authors

Ed Amoroso
Senior Advisor, Teneo
CEO TAG Infosphere, Inc., Research Professor, NYU and Senior Advisor to Teneo Risk

Courtney Adante
President, Teneo Risk Advisory
Teneo Cybersecurity Client Lead and Cyber Crisis Management Advisor

Teneo®
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,600 employees located in 40+ offices around the world.

teneo.com

About TAG Cyber

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 500 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth guidance, market analysis, consulting, and personalized content based on thousands of engagements with clients and non-clients alike – all from a practitioner perspective.

tag-cyber.com