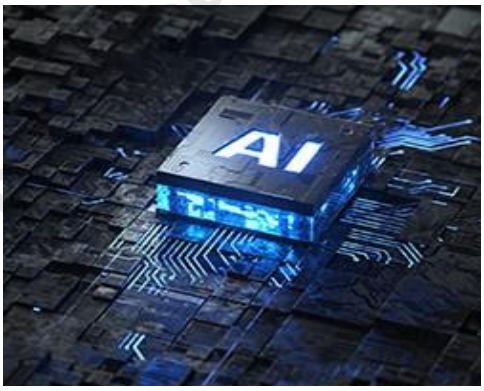
www.pipelinepub.com
Volume 20, Issue 10

Smart AI Ops for IT

By: Mark Cummings, Ph.D.



The advent of PC's with built in AI added to the existing online AIs is creating new challenges for IT Ops. The recent announcements of Co-Pilot from Microsoft, Gemini from Google, AI embedded in MacOS, plus the ability to run GenAI on PC's, promise productivity increases but open the door to new vulnerabilities in cybersecurity, privacy, and maintenance of proprietary information assets. In smart organizations IT Ops and senior management need to partner in developing solutions that will maximize the benefits for AI while protecting the organization.

In most organizations IT is responsible for configuring staff PCs. How phones are handled varies. Some companies provide phones for some or all staff configured by their IT people. Others use a BYOD (Bring Your Own Device) policy with configuration requirements. Others just stay with BYOD. Senior management typically only gets involved at the level of setting objectives in costs, cybersecurity, and ease of use. IT has the sole responsibility of turning those objectives into standard configurations and processes to deploy those configurations. AI is going to require management and IT to do more.

At a high level, the use of AI, while creating benefits in productivity, also creates risks in cybersecurity, IP leakage, and privacy. This means that management is going to have to identify specific job functions and data sets where the risks are too high for those functions/data to be associated with AI. Then, IT ops is going to have to develop AI protection configurations, processes, and procedures for those functions and data sets.

AI Risks

Google has issued a specific warning. It says that Gemini will maintain confidentiality of information put into it by end users. But, it warns that all such information will be used for AI training. The training activity can become a conduit for Intellectual Property (IP) leakage. So, Google says, don't put anything in that you are concerned about leaking.

For example, what this means is that specific proprietary information about an upcoming advertising campaign that company X is working on will be kept confidential. Bu because it is fed into the training, a competitor who asks how to effectively compete with company X may get a plan that doesn't reveal the specifics about company X's upcoming advertising campaign, but does include a plan that effectively responds to it.

Google is clear about using the data. Others are not clear. Still others promise not to use the data. But one wonders. Can they be believed? Finally, we learned in the dot com bust that companies in bankruptcy do sell user data even when they are contractually bound not to. And not all of today's GenAI companies will be around tomorrow. So, it pays to be cautious about data leakage — no matter what.

Microsoft Co-Pilot captures every key stroke and every screen image for the last 30 days on a a PC it is active on. Microsoft says that the resulting data set is encrypted. It also says that the resulting AI system can find anything. Answer questions like, what was that memo from senior management about security precautions I saw a couple of weeks ago? Or, what was the competitor's web site I looked at three weeks ago that said that it had product Y? This kind of support is very attractive.

Unfortunately, there has been a stream of published material on how that data can be accessed by malicious actors. Microsoft has responded by double encrypting the data. The problem is that there are a number of ways that have been published whereby an attacker can gain access to the Co-Pilot app itself and exfiltrate data that way. There are also reports of GenAI systems being used to create cyber-attacks that are both novel and very effective. So, once sensitive data is in Co-Pilot, it may be exposed.

Apple has announced a set of AI enhancements to its O/S and suite of office programs. The enhancements run on both Macs and iPhones. They are less intrusive than Microsoft Co-Pilot and Apple promises strong security and privacy controls. How well they will work has yet to be determined. Elon Musk says he will not allow any Apple computers with AI in the O/S to come into any of his companies. Others have similar concerns.

Central site GenAI systems have, for some time, been seen as capable of generating very effective cyber-attacks. Those attacks have ranged from introducing malicious code to social engineering attacks in the form of fake video calls from the CFO. Operators of central site AI systems have attempted to put controls in place to limit such malicious activity. Their guard rails, however, have had limited effectiveness. Moreover, as GenAI moves out of central sites onto edge systems the ability to use them to create attacks will increase. For example, there is a report of a social engineering attack that cost $10.5 million where it appeared that the CFO was on a video call giving wire transfer instructions.

IT Actions to Minimize Risk

In general IP leakage can be a serious concern depending on the job function and the type of data being handled. This means that a one size fits all set of end point configurations doesn't work. IT has to engage senior management to get a cross section of functional units in the organization to identify the types of data that must be protected from IP leakage and the functions that work with that data.

Once there is a map of functions and data to be protected, senior management must explain to the whole organization what steps are being taken to maximize the benefits from AI while limiting the risks. It is important that all members of the organization understand the situation and support the initiative that senior management is leading. With that in place specific steps can be taken to limit IP leakage. The Gemini warning is a good general caution. Any online AI system is likely to use any input data for training. Other companies may also not be so careful about protecting raw user information. So, guarding against IP leakage can be important. For access to online public systems, certain functions and staff handling certain data may be restricted from accessing public online AI systems. Staff cooperation can be enhanced by IT working with security operations to block access to external online AI systems for those end points used by those staff members.

Some may think that internal, private online company AI systems don't share in this risk. Not necessarily so. If the internal system is built on a platform that a vendor provides which takes user input for the vendor to train with, the same risk is apparent there. If that is the case, IT must treat these systems as if they were external public ones.

Another risk with internal AI systems involves the ones used to help organization members find documents. In these cases, all the organization's documents are fed into the system. This makes that system an attractive attack target. IT needs to work closely with security to add extra layers of protection and monitoring and fast response to attacks.

Instead of private online AI systems, IT may deploy LLM (large Language Models) in personal computers. If done with procedures that erase and then reinstall the LLM's after use, the IP leakage problem may be well contained.

End point AI systems such as Microsoft's and Apple's are in their infancy. It may well be that the IP leakage and cyber security vulnerabilities we see today will be minimized or eliminated in the future. But for now and the foreseeable future, IT needs to develop and deploy a portfolio of end point configurations for very sensitive functions, or for people handling very sensitive data, with no need to deploy AI. For example, this means for high risk functions or data, turning off and de-installing Microsoft Co-Pilot and not allowing the Apple OS containing AI to be installed. For moderate risk functions and data, this means turning off Co-Pilot, but not necessarily de-installing it. Until there is a better understanding of Apple's implementation of AI, it is too early to have specific recommendations for moderate risk functions and data.

Some may suggest that VPN's (Virtual Private Networks) will help with this. Although VPN's can provide some level of security and protection against IP leakage, it is not clear how much. Attackers have found ways around VPNs, and IP leakage out the back door of AI systems may circumvent VPNs.

Phones can be a problem because of BYOD, and IT needs to take steps in this domain as well. With organization-provided phones, IT can provide a controlled configuration. With BYOD phones, IT may need to restrict access unless configuration standards are maintained.

For low-risk functions, organization members may be encouraged to use AI wherever they feel it will improve productivity. There are some functions where actually installing a full LLM will make sense. One such functional area that is receiving a lot of current attention is Customer Service. For some organizations, it may make sense for IT to provide each customer service agent with an end point system that includes a full LLM that can help them with their job.

Managing Risks from Other Companies Integrating AI

Because of the AI imperative, other vendors of hardware and software may feel impelled to integrate AI into their products. Right now, every organization that does so trumpets it. So, it is relatively easy for IT to track these and implement protections.

What do you do if you have taken good precautions, but a supplier or customer has not? This is likely to happen. This means that IT needs to re-examine APIs and messaging interfaces to check to make sure that information that might leak to AI's is controlled. It may be that control is the best that can be achieved in such cases because the data inherent to the functioning of the organization has to flow. In such cases good communication and coordination between organizations may help.

Over time, it is possible that AI "upgrades" may be introduced without notice by vendors with products already installed. IT must be careful and check all updates to identify and respond to new AI insertions.

Responding to Growing Cybersecurity Threat

The same kind of analysis of functions and data sets to identify those of high value and risk should be done for cybersecurity threats, especially from GenAI turbocharged social engineering. There may be refinements to policies and procedures that can lower risk somewhat. Good communication between IT Ops and Security Ops can also be very helpful. But, in the long run, new tools to meet the threat are

needed. Existing tool vendors are struggling to catch up with GenAI threats. It is good practice at this point to identify and partner with new entrants who have tools specifically designed to meet this new threat environment.

Government Regulation Likely

Finally, it is likely that government recommendations, frameworks, regulations, etc., may appear in this area. IT needs to monitor the government situation so that it can respond in such a way as to keep the organization both safe and in conformance.

Conclusion

The advent of PC's with built in AI added to existing online AIs is creating new challenges for IT Ops. The recent announcements of Co-Pilot from Microsoft, Gemini from Google, AI embedded in the MacOS, plus being able to run GenAI on PCs promise productivity increases but bring new vulnerabilities in cybersecurity, privacy, and maintenance of proprietary information assets. In smart organizations, IT Ops and senior management need to partner in developing solutions that will maximize the benefits for AI while protecting the organization.