ACC DOCKET

INFORMED. INDISPENSABLE. IN-HOUSE.

AI — Cybersecurity Solution or Threat?

Compliance and Ethics

Information Governance

Technology, Privacy, and eCommerce

Banner artwork by Ico Maker / *shutterstock.com*

Cheat Sheet

- **A new digital topography**. AI (artificial intelligence) upheavals are changing both how organizations can protect themselves and what they need to protect themselves from.
- **Strength in multidisciplinary harmony.** The intersection of AI and cybersecurity is complex and sensitive, so it is important to stoke conversations with expert voices from various domains.
- **Drafting, rehearsing, and being resourceful**. It is imperative that organizations have a robust, well-tested cybersecurity game plan enriched with all available resources.
- **You are not alone.** Various government programs exist to elevate and guide organizations through cyber-incidents.

We were recently asked whether artificial intelligence (AI) poses a threat to cybersecurity, or whether AI is instead a solution to cybersecurity vulnerabilities? The truth is that AI is not merely one or the other. AI is, in fact, both a threat and a solution to today's cybersecurity concerns. A recent article's title highlights this irony: "The Only Thing Stopping AI Ransomware Attacks is AI Expertise!"

In this article, we give some examples of how AI and cybersecurity intersect in our modern world, including common tools of cybercriminals such as deepfakes. We also share five practical tips for leveraging technology to avoid becoming a cybercrime victim. In short, we strongly recommend that organizations leverage both AI and cybersecurity as part of their overall strategies.

Offense vs. defense

Everybody knows that a successful strategy requires a good offense and a good defense. When it comes to technology, many organizations — including corporations, government agencies and nonprofits — are focused on leveraging AI to gain competitive advantages. This is a smart approach because AI can often be used to increase efficiency, improve operations, and reduce costs. AI can tackle and perform many tasks better than humans, including rapid computations and analysis of large amounts of data. With the power of machine learning, AI can often improve operations and outpace humans. In short, AI is the "offense" for many organizations who want to leverage technology to stay ahead of their competitors.

> AI commonly appears in various forms: the algorithms that power Google searches, Netflix recommendations, and Amazon purchases.

But using AI also carries risks, and the largest risk typically posed by AI is increased cyber vulnerability. AI requires computing capabilities, including access to data, AI algorithms, and increased internet access. These all create (or increase) cyber vulnerabilities for organizations. Some cybercriminals want to sneak into networks to covertly steal trade secrets or data, while others want to blatantly disrupt or freeze systems with ransomware. In all cases, AI increases exposure and provides cybercriminals expanded avenues for cyber intrusions, privacy breaches, and data manipulation.

Unfortunately, many organizations don't realize the vulnerabilities that come with leveraging AI and fail to adequately consider these risks and integrate cybersecurity into their overall strategies. For many, cybersecurity is simply an afterthought, rather than a well-planned defensive strategy. Organizations benefit when they nest cybersecurity strategies with their AI adoption. The key takeaway is that organizations should aggressively leverage both AI initiatives and cybersecurity tools as part of their overall strategies to maximize their performance and success.

AI and cybersecurity examples

AI commonly appears in various forms: the algorithms that power Google searches, Netflix recommendations, and Amazon purchases. But AI can also be used maliciously. AI is the driving technology behind cyberattacks such as ransomware. One author stated that "cybercriminals are also studying AI to use it to their advantage — and weaponize it."

> Humans outperform computers and machines in some tasks such as judgment, common sense, and leadership. However, machines outperform humans in other tasks such as digesting large quantities of data, rapid computation, and completing boring repetitive tasks.

AI is also the power behind deepfake technology. Deepfakes started as Hollywood special effects, but they have evolved and drifted well outside the entertainment industry. Deepfake technology is now readily available to any basement dwelling teenager. Deepfakes have become a common tool of cybercriminals and can lead to catastrophic, multi-million dollar corporate losses.

Deepfake videos can be even more convincing. For example, there are realistic videos of actor Tom Cruise performing magic tricks, but they are totally manufactured. Some have also seen the deepfake video created by Massachusetts Institute of Technology (MIT) students showing President Richard Nixon consoling America after a failed moon landing. It is a compelling video, full of emotion from a grieving president, even though it is obviously a fake.

These extremely realistic deepfake videos can be used for sinister purposes like undermining our judicial systems and threatening global stability. Deepfake technology could be used to fabricate evidence in courtrooms or manufacture propaganda about world events. The inseparability of global security, judicial integrity, and economic prosperity makes this risk particularly concerning.

5 practical tips for leveraging technology

AI and other modern technologies can be used to both benefit and harm organizations. Therefore, CEOs and other key leaders need to understand the benefits and risks to protect their organizations. Organizations should employ human-machine teaming, build multi-disciplinary AI teams, plan for the worst, test cyber response plans before an incident, and leverage government resources. These five tips are outlined below:

1. Employ “Human-Machine Teaming”

AI is a powerful tool, but it cannot solve every problem, nor can it completely replace humans. My number one recommendation for organizations leveraging AI is to employ “human-machine teaming” to get the most out of each. Humans outperform computers and machines in some tasks such as judgment, common sense, and leadership. However, machines outperform humans in other tasks such as digesting large quantities of data, rapid computation, and completing boring repetitive tasks. The key to successfully adopting AI is to combine humans and machines in a way that leverages the respective strengths of each.

2. Build multi-disciplinary AI teams

Leaders should also build multi-disciplinary AI teams. These teams should have executive-level support and “include technical experts such as coders and data scientists, as well as lawyers and AI ethicists, to effectively integrate AI into their organizations. These teams would enable all parties to provide input from their respective perspectives at all stages in the adoption process.” This approach has been leveraged by several large companies, such as Microsoft, and government entities such as the US Army. It is a useful model for other organizations adopting AI. The US Cybersecurity Infrastructure Security Agency (CISA) specifically recommends that CEOs and other leaders empower their Chief Information Security Officers (CISOs) to leverage their cyber expertise.

3. Plan for the worst (Go “Shields Up!”)

Following Russia’s invasion of Ukraine, the CISA recently warned all organizations to go “Shields Up” when it comes to cybersecurity, because “[e]volving intelligence indicates that the Russian

Government is exploring options for potential cyberattacks. Every organization — large and small — must be prepared to respond to disruptive cyber incidents."

Organizations must be ready with a cyber response plan. If they wait to develop a response until a cyberattack occurs, it will be too late. What should this plan include? CISA provides an exceptional checklist to help organizations get started, including a step-by-step guide to "Ransomware Response." The UK's National Cyber Security Centre (NCSC) provides similar resources, including "significantly expand[ed] services to protect UK from record number of online scams."

It is also worth noting that an effective cybersecurity plan requires the use of cybersecurity software powered by AI. Cybercriminals use AI to rapidly identify and exploit vulnerabilities. Law-abiding organizations should use AI-powered cybersecurity tools, because only AI can detect vulnerabilities and then design and employ patches at the speed required to counter the threats. Popular cybersecurity companies such as Sparkcognition, Tenable, and UK-based Darktrace all advertise their ability to leverage AI to counter and stay ahead of emerging cyber threats.

4. Test cyber response plans … before an incident

Developing a cyber response plan is a great first step, but organizations need to test the plan. This will allow the team to identify potential issues and refine the plan *before* a cyber incident. The test should include protecting the "organization's most critical assets in case of an intrusion, including disconnecting high-impact parts of the network if necessary." CISA recommends that senior management — including the C-Suite and board members — "participate in a tabletop exercise to ensure familiarity with how your organization will manage a major cyber incident, to not only your company but also companies within your supply chain." These key individuals need to understand the plan, and their respective roles. Remember the adage: "practice makes perfect."

5. Leverage government resources

CISA and NCSC have many resources to help organizations prepare for and avoid cyberattacks. These organizations can also provide tremendous resources to respond to attacks. Assistant Secretary of US Homeland Security Rob Silvers was a keynote speaker at the 2022 Cybersecurity Summit hosted by the Association of Corporate Counsel (ACC) Foundation. He repeatedly emphasized the importance of leveraging government resources, particularly federal law enforcement, in response to cyberattacks.

> The key takeaway is that organizations should aggressively leverage both AI initiatives and cybersecurity tools as part of their overall strategies to maximize their performance and success.

Interestingly, CISA urges organizations to "lower reporting thresholds" and "consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants." This should encourage companies to overcome their reluctance — perhaps driven by embarrassment or fear of bad publicity — to seek help from law enforcement. The NCSC provides a comparable outline for UK government assistance to guide UK companies through cyber incident responses. In our global economy, companies should leverage this valuable help.

US - Cybersecurity Infrastructure Security Agency (CISA)

UK - National Cyber Security Center (NCSC)

Modernize and protect

Artificial intelligence is a serious threat in today’s cybersecurity setting, but it can also be used to help resolve cybersecurity concerns. Responsible organizations should leverage both AI and cybersecurity as part of their strategy to modernize and protect themselves. They should develop and rehearse response plans for potential cyberattacks. These daunting tasks are made much easier by assembling in-house experts and leveraging external cybersecurity resources, such as those provided by CISA and NCSC.

Patrick Huston

Cybersecurity Advisory Board Member

Association of Corporate Counsel

R. Patrick Huston is a retired Brigadier General in the US Army, where he was the commanding general of the federal government's only ABA-accredited law school. He is a technology lawyer who focuses on artificial intelligence, cybersecurity and other emerging technologies. Patrick is a member of the National Association of

Corporate Directors (NACD). He serves on the Association of Corporate Counsel’s (ACC) cybersecurity advisory board and lives in San Francisco.

Natalie Pierce

Partner

Gunderson Dettmer

Natalie Pierce is a Partner at Gunderson Dettmer in San Francisco, and chair of the law firm’s labor & employment practice. She focuses on the needs of start-ups, emerging growth companies, venture capital firms and private equity funds. She also counsels companies developing and/or incorporating robotics, biometrics, telepresence, artificial intelligence, and other enhancement technologies into the workplace. Natalie hosts the *FutureWork Playbook* podcast, and was selected as Fast Case 50 Award Winner, one of Daily Journal’s “Top Artificial Intelligence Lawyers” and “Top Labor and Employment Lawyers,” Chambers USA’s “Minority Lawyer of the Year,” American Lawyer “Best Mentor,” and San Francisco Business Times “Bay Area’s Most Influential Women.” Natalie earned her bachelor’s at the University of California Berkeley and her law degree from Columbia University School of Law.