Cybersecurity in the Digital Age

BY LINDA SHAVE, LIFE FRIM

Thanks to the internet and modern technology cybercriminals and hackers can reach across the globe and tap you on the shoulder with a digital finger, spreading malware, viruses and bad bots.

All such attacks are aimed at infecting your systems and stealing information as part of their cyberattacks. The value to these cybercriminals and hackers come from stealing information, compromising business operations or holding your data hostage.

"Cybersecurity needs to be part of the fabric of every company and every industry, integrated into every business process and every employee action. And it begins and ends at the top. It is job number one." - ***Charles W Scharf, President/CEO Wells Faroo & Company.***

Interconnectivity between sensors, information sources, enterprises, individuals and the metaverse world is collecting gargantuan amounts of data daily and providing opportunities for cybercriminals and hackers. The exponential growth globally of macro-technology trends such as artificial intelligence, machine learning, generative AI, fake news, data analytics and algorithms has provided a ubiquitous amorphous landscape fuelled by the continued evolution of cybercriminals and hackers who engage in cybercrime.

We could say that cybercriminals are like spies who want government and business secrets, they are the organised criminals who want to steal our identities and money. Cybercriminals include hackers who want to make a political or social statement and terrorist who want to attack our infrastructure.

NAVIGATING THE EVOLVING LANDSCAPE OF CYBERSECURITY

Navigating the evolving landscape of cybersecurity requires agility, scalability and adaptability this is essential especially in areas such as national security where cyber threats continually mutate and evolve. Cybersecurity is not new and IT departments have been using Artificial Intelligence (AI) driven cybersecurity tools and solutions for some time. Original AI driven defence cybersecurity tools and solutions have been designed to protect business from cyberattacks and hackers and offered a significant advantage by automating routine security tasks that required considerable human effort. Activities such as continuous monitoring of network traffic, identifying vulnerabilities, and applying security patches have been handled competently and efficiently by AI driven defence cybersecurity tools.

In general, organisations have taken steps to protect their data and information assets from being accessed via vulnerabilities in its networks and/or business systems. Employees and business regularly changed passwords and understand their responsibilities for protecting business systems from unauthorised access.

However, there is a new and evolving threat on the cybersecurity horizon! AI driven defence cybersecurity tools are now being turned into potential weapons.

The arrival of Generative AI has provided a weapon to manipulate and control machines, provide erroneous information to human operators without their knowledge thus providing fake information, disinformation and malinformation which in turn can potentially harm individuals, citizens, government and business enterprises.

"...there is a new and evolving threat on the cybersecurity horizon! AI driven defence cybersecurity tools are now being turned into a potential weapon."

Cybercriminals and hackers are harnessing the power of generative AI to create more superior and evasive malware software that is specifically designed for cyberattacks. For example, generative AI malware explicitly designed to generate convincing phishing messages that are tailored to exploit network and individual vulnerabilities by creating deepfake. Deepfake and AI chatbots are both products of generative AI and have the potential to create something that does not exist. Generative AI poses not only a great risk to identity theft it is also a threat to cybersecurity.

SO, WHAT IS GENERATIVE AI? A BRIEF HISTORY.

Interestingly, the concept of Generative AI is not new. Around 1932 Georges Artsrouni invented a machine that he called the "mechanical brain" to translate languages. The mechanical translator was a multilingual dictionary which was encoded onto punch cards. In 2006, Data scientist Fei- Fei Li set up the ImageNet database that laid the foundation for visual object recognition. In 2011, Apple released Siri, a voice-powered personal assistant that generated responses and took actions in response to voice requests.

In 2014, Ian J. Goodfellow and colleagues published the first paper on Generative Adversarial Networks (GANs) which is a class of machine learning frameworks for approaching Generative AI, the aim being to determine if an image is real or fake and in 2022, we saw the arrival of ChatGPT.

It is hard to believe that the introduction in late 2022 of ChatGPT (which provided a chat-based interface to its GPT 3.5 language learning model (LLM)) could have had such an impact and start the race for the creation of generative tools. These generative tools have transformed how people search, use and assess information. Although tools such as ChatGPT can respond coherently the outcome is not always accurate.

The consequences could result in disinformation, malinformation and the possible generation of hate speech all of which could cause geopolitical crises.

Spanning the years 1932 to 2024 generative AI has excelled in recognising images, classifying articles and converting spoken words into written text. In essence generative AI can create synthetic images when given a description, generate papers about a particular topic or produce audio versions of written text as well as creating video images of a person and using their voice to create fake imposters and even write computer programs.

In the context of cybersecurity generative AI has the potential to enhance the ability of bad actors to flood us with fake content masquerading as truth and fake voices that sound eerily like those of our loved ones. Can we trust what we see or hear? The answer is probably not. In the wrong hands generative AI tools could cause even worse problems launching cyberattacks or causing havoc in energy grids, financial markets, information transmitting technologies and communication infrastructures. Generative AI language learning models continue to learn and thus the generative AI tool might become capable of making plans on their own and acting on them. Generative AI raises potential risk to infrastructure, data, people, applications and algorithmic risks.

SO, WHAT IS THE METAVERSE?

The metaverse is a seamless convergence of our physical and digital lives, creating a unified, virtual community where we can work, play, relax, transact and socialise. An outcome of COVID-19 was the acceleration of digitisation, online engagement, communication and virtual experiences. The metaverse world continues to evolve with Augmented Reality (AR) and Virtual Reality (VR) headsets providing a powerful user experience. Use cases include online working and education which can now be conducted through video calls and virtual social events. The metaverse enables people to immerse themselves into education and learning, have access to remote healthcare, government services and shopping experiences without the geographical restrictions. However, in this metaverse world which is collecting gargantuan amounts of data daily there is the potential of vulnerability risks such as data privacy, user health and safety, secure identities, fraud and cybersecurity.

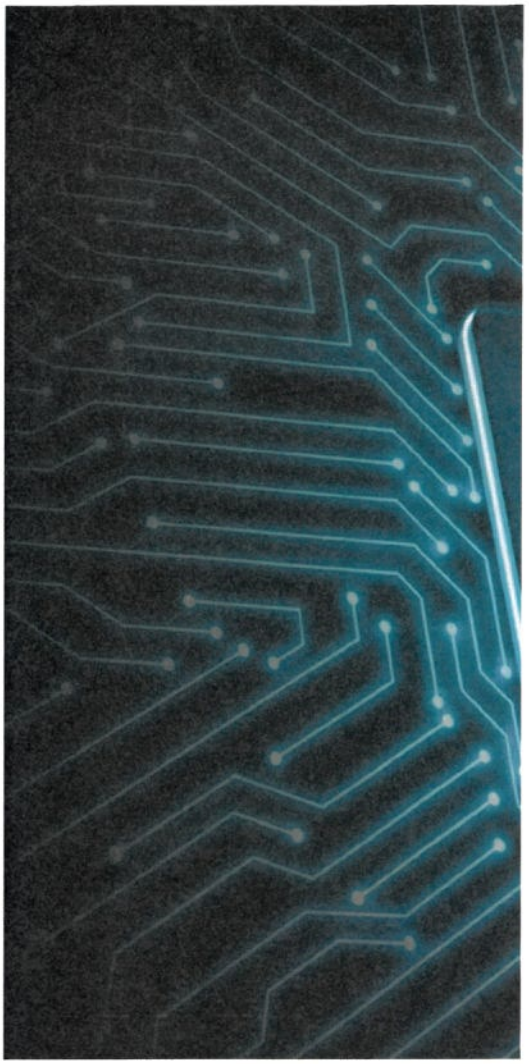
ADDRESSING EMERGING CYBER THREATS AND VULNERABILITIES

Addressing emerging cyber threats and vulnerabilities requires understanding that originally AI driven defence cybersecurity tools have been designed to protect business from cyberattacks and hackers. Times are now changing as AI driven defence cybersecurity tools are now being turned into a potential weapon with the rise of generative AI technologies. The arrival of generative AI has provided a means to manipulate and control machines, provide erroneous information to human operators without their knowledge thus providing fake information which, in turn, can potentially harm individuals, citizens, government and business enterprises. Another threat area for consideration might include 'anonymisation'. Anonymisation or de-identification is the process of removing as much data as possible that relates to individuals for example names, addresses and other identifying features that might identify an individual. This is particularly important in the era of government and business who are sharing large quantities of real time data. However, artificial intelligence, machine learning, algorithms and pattern recognition artificial intelligence tools can be effective at adding data features back into datasets, by for example, cross-referencing other available datasets. This in turn could pose a cybersecurity risk as well as exposing inadvertently information that might identify an individual.

It is interesting to note that governments and private enterprise services are asking customers to use voice recognition, thumb prints or biometrics as a safeguard to accessing customers services and their personal information. However, these blueprints of your biometrics and voice can now be used against you with the rise of generative AI technologies that can use your voice and features to create a fake 'you'. One therefore needs to ask the questions how safe is your information?

And if stolen, how safe are you against being exploited or your identity, private information and any sensitive data being used against you? These are crucial questions for every citizen, government and private enterprises need to be able to answer how they will manage this superior and evolving cybersecurity mine field of cybercriminals, hackers and generative AI. Government and private enterprises need to convince every citizen and individual that they can be trusted to protect you from cybercriminal threats, fake news, disinformation, malinformation and identity theft.

"In the wrong hands generative AI tools could cause even worse problems launching cyberattacks or causing havoc in energy grids, financial markets, information transmitting technologies and communication infrastructures."



SO, WHAT IS FAKE NEWS?

Fake news also sometimes referred to as the deepfake universe has escalated since the arrival of generative AI tools and the rise of disinformation and malinformation So what is disinformation and malinformation?

What is Disinformation?

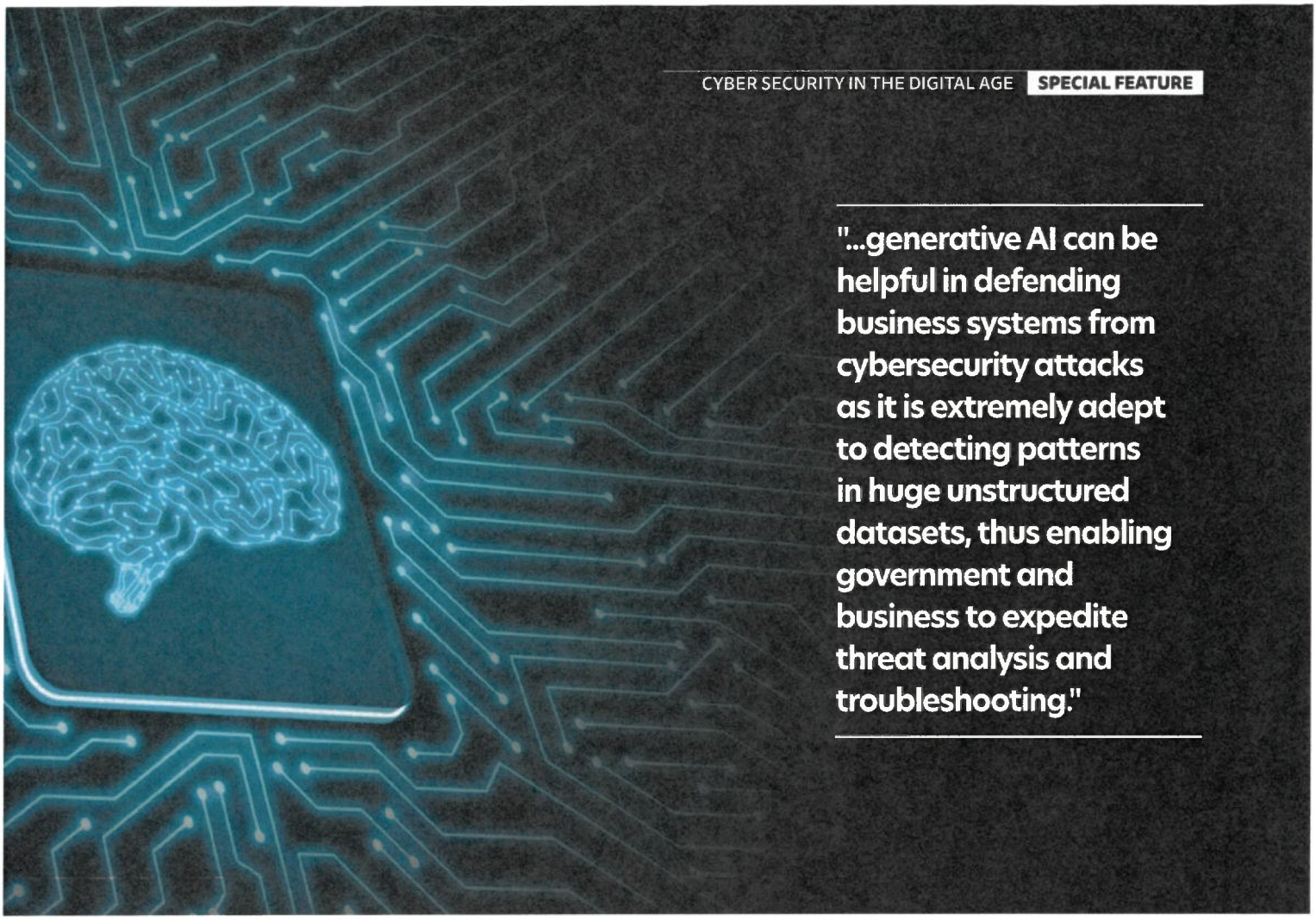
Disinformation is false or inaccurate information that is deliberately created and spread to harm a person, social group, organisation or country.

What is Malinformation?

Malinformation is accurate information inappropriately spread with the intent to cause harm, particularly to the operation of democratic processes.

Therefore, when addressing cybersecurity, emerging cyber threats and vulnerabilities in networks and business systems government and business need to consider in their cybersecurity strategies and policies:

- How do we identify fake from real information?
- How do we identify that data and information is trustworthy, ethical, non-bias, honest and righteous?



"...generative AI can be helpful in defending business systems from cybersecurity attacks as it is extremely adept to detecting patterns in huge unstructured datasets, thus enabling government and business to expedite threat analysis and troubleshooting."

BEST PRACTICES FOR SAFEGUARDING SENSITIVE INFORMATION

To address emerging cyber threats and vulnerabilities, record and information management professionals need to understand the difference between information security and cybersecurity. Information security and cybersecurity are terms used interchangeably because in their basic form they refer to the same things, which is protecting the availability, confidentiality and integrity of data.

However, there is a crucial difference:

- Information is at the heart of the organisation, whether it is a business record, personal data or data collected as an outcome of a transaction. Information assets can be collected, secured, managed and kept in an electronic document and records management (EDRM) system or other business systems. Information security protocols are normally placed at the point of creation, capture or scanning and registering the information asset (data) into your EDRM systems or business systems. Information security focus is on protecting data from loss, unintended or unauthorised access, use or sharing.
- Cybersecurity on the other hand covers the steps an organisation takes to protect its data/information assets that can be accessed via vulnerabilities in its networks and/or business systems. Cybersecurity focus is on safeguarding data from cyber-attacks, external malicious breaches, inadvertent internal breaches and/or third-party partner breaches.

The primary challenge and risks will be how to safeguard the omnipresent technology, networks, sensors and the Internet of Everything against generative AI cyber-attacks, data loss and privacy breaches. It maybe noteworthy to mention that every smart grid, sensor for smart streetlights, traffic lights, surveillance monitoring devices etcetera, all have their own Internet Protocol Address (IP) which uniquely identifies them just like your internet, mobile (cellular) phones, wireless-enabled laptops, smartphones and tablets IP addresses identify you.

If we consider that for every individual who is wirelessly connected and all the sensors across a city, state or the globe there are billions of discrete end points and IP addresses. In fact, one might ponder that over time in the omnipresent wireless connected world there are now more sensor IP addresses in smart cities, smart devices and objects than IP addresses held by individual people.

Some best practices for safeguarding sensitive information might be to instigate a managed vulnerability rationalisation and business impact analysis by utilising cyber digital twins. A digital twin platform can help the business in identifying how they capture data, visualise business processes, simulate different scenarios, discover business operational critical assets and enable the organisation to analyse and secure their physical systems and infrastructure. Further, your cybersecurity and information security strategies, policies and procedures need to include how will you manage the risks, how do you measure the outcomes, steps for communicating, ongoing monitoring and reporting.

To err on the side of caution, there are many ISO standards and best practices for addressing cybersecurity. However, as outlined in the above generative AI discussion there is a new level of complexity, generative AI cyberattacks are using large language

models including nefarious acts for sophisticated phishing incidents. The utilisation of third-party datasets, plug-ins and pre-trained models could increase vulnerabilities.

Generative AI may also inadvertently reveal confidential data in its responses, leading to unauthorised data access, privacy violations, and security breaches.

On the positive side of generative AI is that generative AI can be helpful in defending business systems from cybersecurity attacks as it is extremely adept to detecting patterns in huge unstructured datasets, thus enabling government and business to expedite threat analysis and troubleshooting. Government and business will need to consider new approaches for cybersecurity awareness and education for all employees.

INTERVIEWS WITH CYBERSECURITY EXPERTS AND THOUGHT LEADERS

I am deviating from interviews with cybersecurity experts and thought leaders to draw your attention to something much closer to home, the ransomware cyberattacks of a Public Library. The public library was in Toronto where on 28th October 2023 100 branches and nearly 5,000 computers went down resulting in 1 million books piling up in storage.

The ransomware cyberattacks encrypted Toronto Public Library computer systems and stole staff information. The link to the CBA News article posted on 27th February 2024 is a great insight into what happened. It also reflects how staff rallied together by reverting to manual processes just to keep books circulating and services open to the public. The report indicates that Toronto Public Library did not pay a ransom to restore its system, instead they chose to rebuild it themselves. A great read and a real example of resilience in the face of hacker extremism.

See article www.cbc.ca/news/canada/toronto/toronto-library-ransomware-recovery-1.7126412

In ending, there is indeed a lot of food for thought around cybersecurity in our digital world and how we continue to manage the changing landscape and moving goal posts of generative AI.

The topic around the good and bad of generative AI deserves future round table discussions, not only within information management circles but with our colleagues in IT, risk management, auditing and security.

ABOUT THE AUTHOR

Linda Shave FRIM, is acknowledged as a thought leader and architect of change. She is a researcher, consultant, educator and author on topic areas such as intelligent information management, artificial intelligence, robotic process automation, privacy, and security. Linda is a gold laureate winner for Government Innovation and has an interest in data science, robotics, and quantum computing. Linda is a member of numerous professional organisations. Linda can be contacted at linda.bizwyse@gmail.com