

DATA RISK MAGAZINE

Issue No. 1, Halloween 2023

THE THREAT OF VENDOR BREACHES

Can you trust your
service providers?

SCARIEST AI TRENDS IN CYBERCRIME

The biggest
disruption in
cybersecurity
history

SPOOKY CASINO CYBER CRISIS

Does ransomware
spawn identity fraud?

BEWARE OF KILLER BUNNIES

REAL OR AI?

COMPLIMENTARY
INAGURAL ISSUE



LETTER FROM THE EDITOR

"We live in interesting times", as the saying goes. The Internet used to be a neat invention to keep in touch with colleagues and subscribe to email discussions. Today's digital natives can't imagine a disconnected device, but that's in part because all the fun stuff now happens online.

From awesome deepfakes of Tom Cruise to sinister AI footage of battlefield action lifted from computer games, literally everything from social media to cable news stations is created with one goal in mind: to distract us long enough for the nudge to happen.

Cynics might argue that we now need to choreograph and gamify distractions just to have a meaningful conversation with kids and business associates alike. Our tools became systematic about a decade ago and we saw productivity gains from using technology as an enabler. With artificial intelligence and machine language, our tasks are now automated, and we suddenly seem to be on a collision course with a singularity that was supposed to take another three decades to materialize. Scary enough for you?

Our Spookiest Issue to Date

For our Hallowe'en issue my team and I invite you to enjoy this cybersecurity-themed digital publication. We've built this issue based on content that fascinates us, so we hope you like it. And every once in a while, we hope to pull a rabbit out of a hat, so to speak, and surreptitiously add a sprinkle of AI to the mix, but hopefully not so much you'd notice.

Enjoy!

David





THE SCARIEST AI TRENDS IN CYBERCRIME

IS ARTIFICIAL INTELLIGENCE THE NEXT GREAT DISRUPTOR?

ALREADY



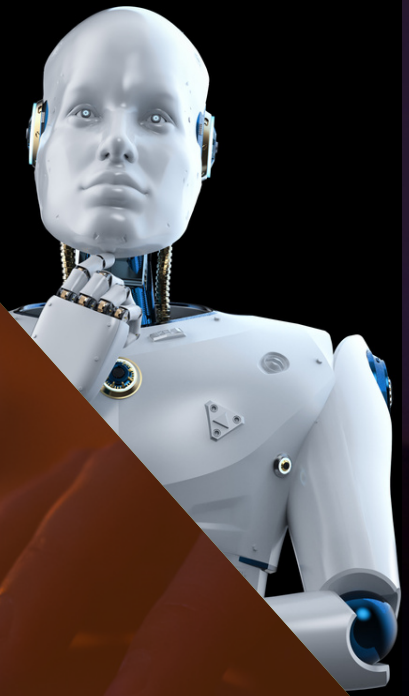
Artificial intelligence (AI) is not just a buzzword, but a reality that is transforming every aspect of our lives. One of the most critical areas where AI is making an impact is cybersecurity. However, this impact is not always positive. In fact, AI is a double-edged sword that can be used for both

good and evil. On the one hand, cybersecurity firms are leveraging AI to create sophisticated algorithms that can detect and prevent cyberattacks, protect sensitive data, and enhance online security. On the other hand, malicious hackers are exploiting AI to launch more powerful and stealthy attacks, breach data privacy, and cause havoc in cyberspace. To avoid these looming threats, first we must understand the emerging threats, analyze their strengths and weaknesses, then develop a plan to defend against them.








THE SCARIEST AI TRENDS IN CYBERCRIME



COULD A.I. GUESS YOUR PASSWORD?

Have you ever opened an account to discover your password has been changed without your knowledge? This is the case of a compromised password. Regardless of the methods used, somebody has discovered your password. This is no new phenomenon, but AI password cracking is a sophisticated method of exposing passwords. Each hacker's motivations are different, but this strategy is typically used to get into accounts, databases, or files protected by passwords. Using various methods, such as trying every possible combination of characters or using common words and phrases, AI algorithms have the potential to crack passwords exponentially faster than

“traditional” hackers. In some cases, Machine learning is used to train neural networks to guess passwords based on data from previous password breaches, increasing their accuracy and efficiency. The emergence of these strategies is scary, but equally preventable when you take the right precautions:

-  Use different passwords for each account. Make each password long and unique.
-  Turn on two-factor authentication whenever possible to add another layer of security.
-  Stay updated on the latest threats in cyber safety and how to avoid them. Don't let hackers catch you off guard.



FREE RESOURCES



THE SCARIEST AI TRENDS IN CYBERCRIME



WHEN A.I. GOES VISHING

The phone rings and it's your good friend, but something feels wrong. Their voice is frantic and for whatever reason, they need money... now. Vishing is a social engineering trick that takes advantage of human nature to steal sensitive information from the victim, but AI impersonation is next-level Vishing. This is a sneaky way of using AI to copy how people talk or sound. Malicious hackers are using AI to make fake calls or messages that sound very real. By using voice and video clips of an individual that exist online, they can create very convincing impersonations of almost anyone. They often target close family members or friends and convince them to send money or personal information, claiming it's an urgent situation. In the hands of a skilled hacker, AI impersonation can

be used to extract sensitive data from corporations or confidential databases, posing as an authorized user. As AI advances, vishing scams are certain to become more convincing. Learn how to protect yourself now and future-you will be grateful:

- 🔊 Don't trust caller ID, it can easily be spoofed.
- 🔊 Never give sensitive information over the phone or online unless you have verified the caller's identity.
- 🔊 Always be skeptical about calls and messages from unverified senders. When in doubt, hang up or ignore it. You can also report the number to authorities.
- 🔊 If you are unsure if a call or message is real, contact the person or organization directly using a different channel.



FAKE BUNNIES ARE JUST THE START

Take a look at the image above. This image was created in a matter of minutes using AI. Now imagine, these same tools can be used to depict real people in fake situations. AI deepfakes are advanced recreations of real people. Hackers collect a variety of data, including videos, images, and voice clips, and then train an AI algorithm to mimic that person's behaviour and physical image. As AI continues to improve, these fakes will become increasingly realistic and hard to spot. AI deepfakes can be used for various malicious purposes, such as spreading hateful messaging through an individual with a large audience. On a smaller scale, AI could be used to replicate a video call from a friend or family member,

attempting to extract money or personal information from the victim. AI Deepfakes are a novel concept, and protecting yourself against them requires a conscious and continuous effort when interacting with the online world:

- 🌀 Don't believe everything you see or hear online without checking the source and the context.
- 🌀 Use tools that can detect deepfakes, by analyzing images or videos and tell you if they are likely to be fake.
- 🌀 Report any deepfake content that you find. If you see a deepfake that is harmful or misleading, you can report it to the platform where you found it or to the authorities.



The age-old adage “The house always wins”, rings false as a major cyber attack leaves Vegas scrambling for solutions.

The Day The Casinos Got Owned by Ransomware

In September, two of the biggest casino chains in Vegas suffered data breaches that exposed thousands of customers' personal data and disrupted the casino's operations and services. These casinos, MGM Resorts and Caesars Entertainment, are no strangers to cyberattacks. Let's look at how this all started.

MGM was targeted by a group called AlphaV, who claimed to use a ransomware service called ALPHV. Ransomware is a type of malware that encrypts the victim's data and demands payment to unlock it. The group said they used a social engineering tactic called "vishing" to steal login credentials from an MGM employee. The employee was able to identify the vishing attack and report it, but not before giving up sensitive information that enabled the company-wide attack. The hackers then used the employee's credentials to infiltrate MGM's network and deploy their ransomware. This serves as a reminder that better cybersecurity training is needed across all sectors of the economy.

Despite the attacks occurring in the same week, Caesars was targeted by another group called Scattered Spider. Notorious for using “double extortion tactics”, threatening to publish their victim's data on the dark web if ransoms are not paid.

Scattered Spider did not reveal how they hacked Caesars Entertainment, but they claimed to use a zero-day vulnerability to exploit their network. This is a flaw in a company's system that is unknown to the vendor or the public, allowing malicious groups to bypass security measures and locate sensitive information before anyone is aware or able to resolve the vulnerability.

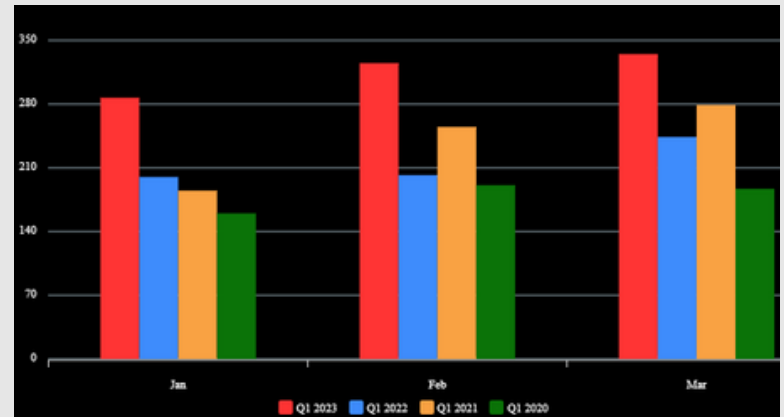
Both MGM and Caesars did not disclose how much data was stolen or affected by the cyberattacks, but it could be substantial. Caesars paid out half of the \$30 million ransom set by the attackers, while MGM has declined payment altogether. It is still unclear whether either casino has recovered its data.

Is Vegas Vulnerable?

Vegas has a long history of cyberattacks. For instance, MGM was targeted back in 2020 by a similar cyber attack that exposed the data of nearly 11 million customers, including celebrities, journalists, and government officials. So why is Vegas a hotspot for cyber criminal activity?

Well naturally, Las Vegas casinos handle an enormous amount of money making them attractive victims for ransom. However, this problem goes far beyond just money. Casinos in Vegas notoriously have weak cybersecurity protections, relative to other companies today with similar revenue. An article by Forbes explained that the MGM board of directors is significantly lacking in tech and cybersecurity knowledge, despite them being directly responsible for the digital security of the business. Finally, casinos are likely to have a vast selection of data points for each of their customers, which is especially useful for hackers hoping to extract a ransom payment from them.

This unique set of circumstances positions Vegas casinos as a popular target for cyberattacks. These attacks of course pose a threat to large casinos like MGM, but these businesses can typically survive a cyberattack using their vast wealth. Unfortunately, the same cannot be said for many other industries and businesses that are often victims of cyberwarfare.



Data breaches of notable companies like MGM and Caesars often bring ransomware attacks to headline news, but they are far from the most vulnerable sectors and organizations that are unable to pull the same mainstream attention.

Industries that store lots of sensitive customer data are always attractive targets for ransomware attacks. Small medical practices, local government offices, and small businesses are frequent targets, yet it's rare for a major news outlet to bring awareness to these smaller-scale attacks. In many cases, these businesses cannot survive a major data breach due to capital constraints, and end up dissolving altogether.

Ransomware attacks are on the rise in 2023, and we must pay more attention to vulnerable sectors to prevent small-scale cyber warfare from flying under the radar. Large breaches are great at bringing mainstream attention, but they rarely encompass the severity of this growing problem. Understanding emerging cyber threats is the first step to implementing an effective prevention strategy.



THE SCARIEST AI TRENDS IN CYBERCRIME



ARTIFICIAL PHISHING

We all know somebody who has fallen victim to a phishing scam before. All it takes is clicking one link and boom, your data is stolen. Phishing email scams have existed since the inception of the internet. AI-generated phishing emails are a more sophisticated version of this age-old scam. Hackers are using AI to write convincing emails that look like they come from someone you know or trust, such as your bank, your boss, or your friend. They use AI to scan the internet and learn about your interests, habits, and writing style, and then copy them to make the emails seem more authentic. They also use AI to create fake websites or attachments that look real but are harmful. If you click on them, you may download malware, lose your data, or be

pressured to pay a ransom. AI-generated phishing emails are more dangerous than regular phishing emails because they are harder to spot and easier to produce. However, avoiding them is no different than avoiding traditional phishing scams:

- ✦ Don't open or click on links or attachments from unverified senders.
- ✦ Verify the sender's identity by using another channel of communication.
- ✦ Carefully check the sender's email address and the website's URL for unexplained differences.
- ✦ Use antivirus software and report any suspicious emails you receive to your IT department or the authorities



FREE RESOURCES



THE SCARIEST AI TRENDS IN CYBERCRIME

CAN A.I. HACK BETTER THAN IT CAN DRIVE?

Although self-driving cars are the future, that's not the kind of AI driving we're concerned with today. Hacking, in the general sense, has existed for a long time. However, AI-driven hacking is becoming more prevalent as the capabilities of AI rapidly improve. This is when hackers leverage AI to automate or enhance the process of finding and exploiting vulnerabilities in systems and networks. Using AI, they can apply reinforcement learning or other methods and train algorithms to learn from their previous attacks, discover new attack vectors, or evade detection by the victim. AI-driven hacking can have serious consequences, such as sabotaging systems, compromising confidential information, or initiating cyber warfare.

These methods have made headlines in recent years as AI has been more effective at hiding its trails in companies' networks and systems than humans have ever been capable. Ensuring cybersecurity requirements and protocols are up to date is the most important step to prevent AI-assisted attacks:

- 🔒 Make sure to maintain your systems with the latest updates.
- 🔒 Use robust authentication methods for all users to provide additional layers of protection.
- 🔒 Consistently and thoroughly monitor your network traffic to detect potential attacks as soon as possible.



FREE RESOURCES

WHAT DOES CANADA NEED TO BE A CYBERSECURITY CONTENDER?

BY TIM KING
CONTRIBUTING AUTHOR

There are countries in the world that should be crippled by cybersecurity compromises but aren't. The countries that take cybersecurity seriously are also the countries that approach it with a wholistic strategy that emphasizes communication, collaboration, and strategic oversight. The nature of cyber crime and espionage is intensely asymmetrical. It's very easy for criminals and foreign powers with ill intent to quietly go about the business of disrupting Canadian interests without any reciprocity. The lack of clear evidence for a cyberattack is one of the main reasons it continues to boom as both a criminal and a political tactic.

The concept of an attack surface is familiar to those working cyber, but it's something the general public should get their heads around too. An attack surface is conceptual and gives defenders and attackers a way to understand the many ways to get into a secured system by representing it as a single entity. The most obvious example of an attack surface would be the electronic devices used and the networks we connect them on. A wired ethernet network has a smaller attack surface than the same system with Wi-Fi enabled because it has less avenues into the network. But attack surfaces exist beyond physical technology; they also exist as the result of policy.



In Canada we have approached cybersecurity in a piecemeal manner, funding competing organizations and often prompting them to repeat (with varying levels of excellence) programs that already exist while ignoring other areas entirely. These organizations compete for funding with no regard for a coherent national strategy. In many cases, the funding itself causes the gaps by creating repetitive programming.

This approach leaves many gaps in our national attack surface, and gaps are where threat actors thrive. If Canada wants to survive and thrive in an increasingly interconnected and volatile world, we need to begin aligning our resources and supporting one another's approaches. This doesn't just mean in government or in industry, but across all sectors. Only through circling our wagons and working together can we hope to defend against attackers who have every advantage in the asymmetrical world of cybersecurity.

CAN VENDORS BE TRUSTED?



Your cyberdefense is only as strong as your weakest vendor.

Insist on these Top 10 security requirements:

- ☑ Proof of Independent Audit
- ☑ Data Flow Policy
- ☑ Incident Response Readiness Plan
- ☑ Employee Training & Awareness
- ☑ Multifactor Access Policy
- ☑ Encryption & Confidentiality Procedure
- ☑ Cyber Insurance Coverage Policy
- ☑ Certified Privacy Officer
- ☑ Supply Chain Security Procedure
- ☑ Privacy Compliance Policy

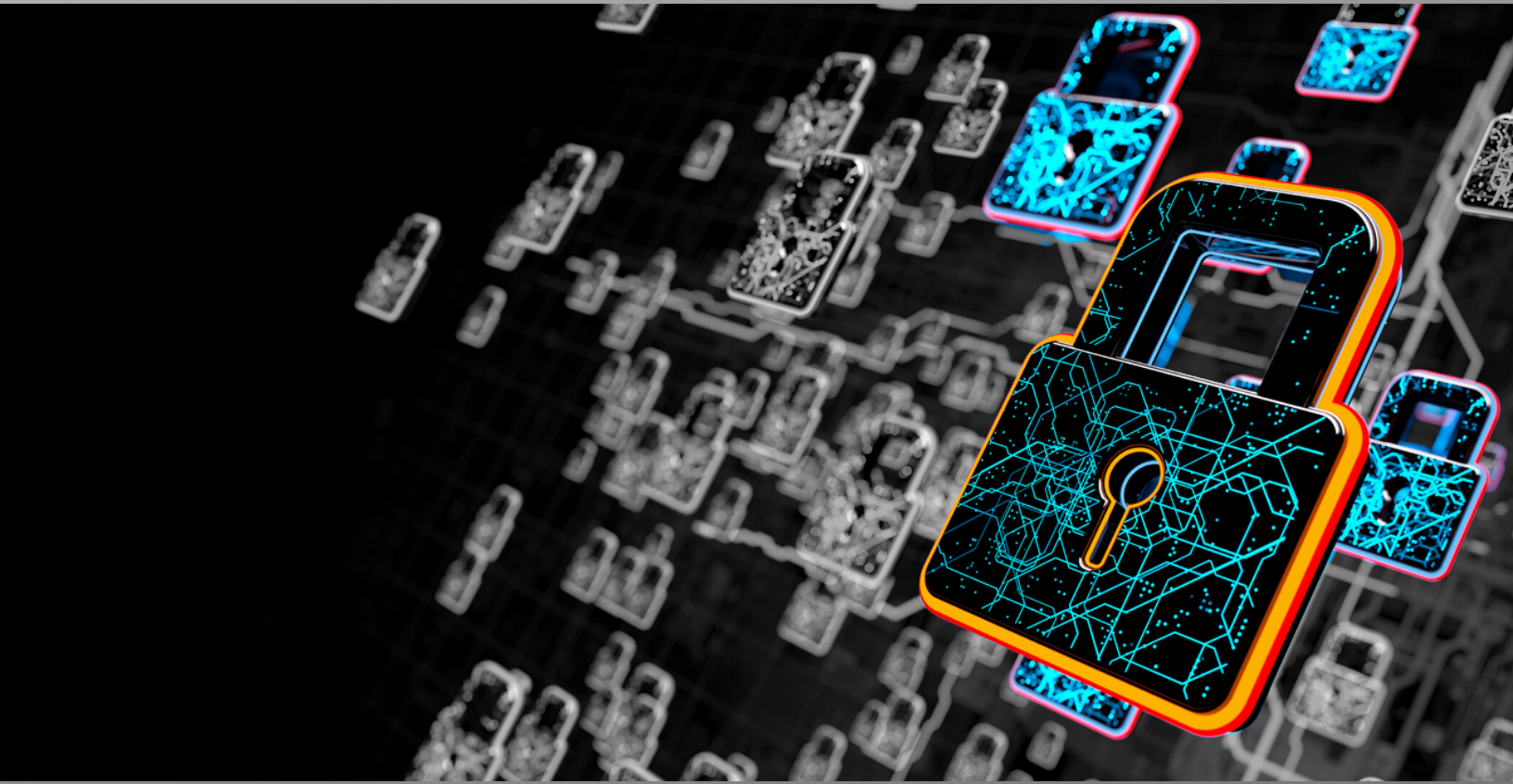


When in doubt, use our handy checklist to lower your risk



**GET THE
CHECKLIST IN
ONE CLICK!**

DATARISK MAGAZINE



We want to hear from you!

- Feedback
- Contributions
- Editorial letters

Reach us at editor@datarisk.ca
with your ideas and reactions!



Issue No. 1, October 2023

www.datarisk.ca

