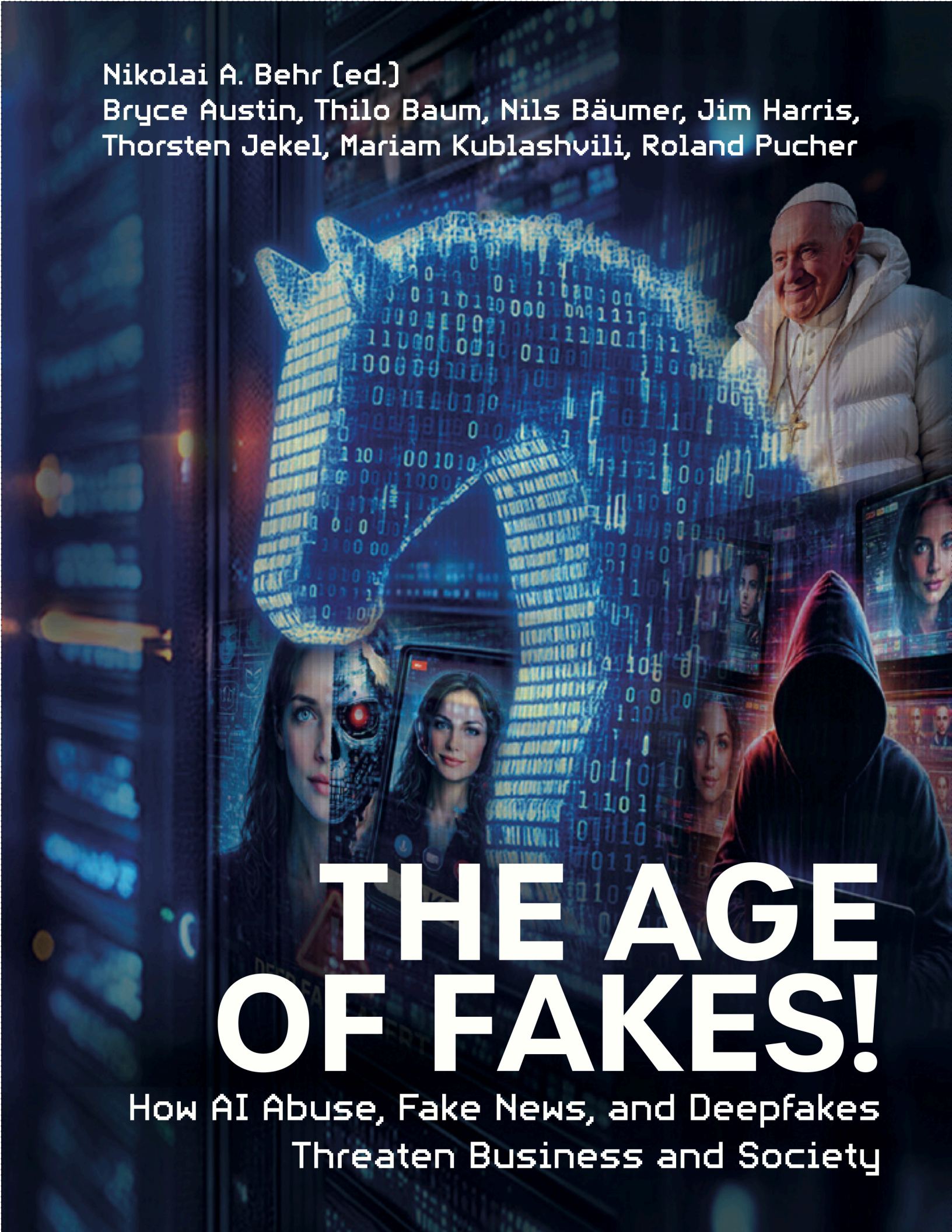
Nikolai A. Behr (ed.)
Bryce Austin, Thilo Baum, Nils Bäumer, Jim Harris,
Thorsten Jekel, Mariam Kublashvili, Roland Pucher



THE AGE OF FAKES!

How AI Abuse, Fake News, and Deepfakes Threaten Business and Society

CYBERCRIME Skyrocketing

Deepfakes & Cybercrime are Intimately Linked
10 Things You Can Do to Reduce Your Risk

By Jim Harris

Cybercrime is costing companies, governments, and citizens trillions of dollars a year globally. Bad actors are increasingly using deepfakes as a means to defraud corporations, institutions, governments and average citizens.

A Cautionary Tale

I was on a TV show talking about artificial intelligence (AI) recently. The host, who is in the public eye, shared an experience. There are hours of video of her on the TV station's site and YouTube. Scammers had trained an AI on her voice. Her family received a phone call that sounded EXACTLY like her that went something like this:

Her family has a safe word. If a family member doesn't use it in this kind of emergency phone call, everyone knows that it's not them. For this example, I'll make one up: "jalapeno peppers." If it'd really been her, she might have said, "I'm in the hospital and am starving and want to have a pizza with "jalapeno peppers." Her family then would have known that it was really her.

"I've had a car accident and rolled the SUV. I got out okay, but the car burned, and my wallet was inside. I'm in the hospital and am starving and the food is terrible. Can you please send $200 right away to nursebetty@gmail.com so that I can get something in the cafeteria?"

So, the question is: Have you done safe word training with your family? Grandparents are particularly vulnerable to this kind of fraud.

Deepfake Video Cost $200M

In February 2024, an accounts payable clerk in the Hong Kong office of Arup, a multinational firm, received an email asking her to join a finance video call from her firm's UK-based CFO. She joined the call with the CFO and several other colleagues in finance. The CFO said something like, "We have a VERY serious problem. We

haven't paid our most important supplier in 90 days. And if it goes one more day, we might lose them. That would be catastrophic. I want you to immediately transfer $200 million to these subsidiaries of theirs in different countries."

So, the clerk made the transfers totaling about HK$200 million (US$25.6 million). After contacting the company's headquarters, she learned that the CFO had never authorised the payments. The fraudsters used AI-generated "deep-fake" videos and cloned voices, not just for the CFO, but for all the other finance department people on the call too.

It Was the Best of Times; It Was the Worst of Times

"It was the best of times, it was the worst of times," is the opening sentence from *A Tale of Two Cities* by Charles Dickens.

We are living in both the best of times and the worst of times today: Never before has humanity had such powerful tools at its fingertips. At the same time, it has given these powerful tools to bad actors, those who are often the fastest to adopt new tools, using them to create convincing deepfake audio and video.

Alarming Media Coverage

Media coverage of deepfakes is overwhelmingly negative (no wonder, given the stories above). I would like to provide some positive examples of the incredible benefits of Deepfakes. First with headshots, then a museum in Florida's application, and finally, a fascinating story about the father of modern psychology.

Headshots: The Real Cost?

Every seven years or so, I get new headshots. It costs me $300 for a photo shoot in a photographer's studio, but that's just the tip of the iceberg in terms of cost.

The photographer will have extra charges based on time, number of changes of clothing, the number of backgrounds that I want and the number of final photos I choose.

Mid-range, off-the-rack, men's suits cost $400 to $1,000, while a Hugo Boss suit will cost up to $1,400, so buying three new suits for the photo shoot can add thousands of dollars of additional cost for new threads.

But the real cost is the time away from the office. I work with the largest CEO peer mentoring group in Canada. A CEO running a $100 million a year business is responsible for $50,000 of revenue every hour. So, four hours for a photo shoot (including travel, buying new suits, setting up) has an opportunity cost of $200,000.

Three AI headshot sites – Aragon.ai, InstaHeadshots.com, and HeadshotPro.com – all received more than 200,000 US visits from October 1 to November 30, 2025 representing more than 90% of the market share according to Semrush. (Semrush is a digital marketing platform for SEO, PPC, content, social, and competitive research providing report insights globally). Aragon has created 39 million headshots, Estonia based BetterPic.io has created 33 million, InstaHeadshots 20 million, and HeadshotPro 18 million.

For all four services, you upload between five and 15 clear photos of yourself, then

you choose attire, backgrounds, and poses. And on a more granular level you can determine your expressions and angles. Standard, basic, and executive packages give you different flexibility and number of headshots ranging in price from $29 to $75.

I speak at conferences and seminars all around the world. Imagine that I was being hired by Sea Ray to keynote at the Sea Ray 65th Anniversary Dealer Meeting in Knoxville Tennessee. The company's Sundancer 320 is the most popular new 30-40 footer sold in the US. If I really wanted to customize my keynote, I'd rent a Sundancer 320 for a few hours and get a few headshots on the boat - or I could just use one of the above headshot services. Same goes for video. Using Sora or Google's VEO3, I could create an image of me out on the water on a Sundancer 320. Here's a photo of my colleague Aidan Crawford, who did exactly this.

"Studio quality headshots, minus the studio costs," is the market line from InstaHeadshots.com and it rings true. But it's not just the cost; it's the convenience, the speed and the flexibility. I can create hyper-realistic, professional, customized headshots in minutes from the convenience of my office desk.

Summary
In summary, it's not just the money. It's about the hyper-customization, the incredible amount of time you can save, the convenience and the flexibility.

Talking To Salvador Dalí

This Museum in St Petersburg Florida Brings Dalí Back to Life

You can talk to Spanish surreal artist Salvador Dalí at the Dalí Museum in St Petersburg, Florida. The museum has brought the famed artist back to life using AI.

The experience began with an 8-foot-high iPad in the lobby in 2019. You could go up to a 3D image of Dalí and take a selfie with him.

The museum upgraded the experience in 2024 by uploading all the video and audio of Dalí and his writing and diaries into OpenAI's ChatGPT4 and then synthesized his voice with ElevenLabs.

The result was that you could ask Dalí anything. Such as: "Why did you paint melting clocks?"

To which Dalí would answer, "To symbolize the fluid, unreliable nature of time, inspired by a dream about Camembert cheese melting in the sun, representing how time softens and loses meaning in dreams and memory." The response is in Dalí's unique, Spanish accent. It's like actually talking to Dalí if he were still alive. If the answer to your question is not directly within the data set, the AI will synthesize the answer of what Dalí would likely have said.

When I was a kid and our family went to a museum or art gallery, we'd rent headsets that came with earphones and as you walked about the gallery you'd enter the number of the painting or sculpture that you were standing in front of and a narrator would tell you the history of the piece.

Imagine how much more engaging it is for children to talk directly with the artist? In a later section I'll discuss how customized AI tutoring will improve learning outcomes by up to 100-fold by 2030.

Teachers today complain that they have to compete against TikTok and Disney for the attention of students. AI and this deepfake example create a level playing field. The Dalí AI is deeply engaging. Teachers and the education system need to embrace this technology.

I called the Dalí museum in researching this piece and asked them to imagine a smartphone app that museum goers could download. 5G is hyper accurate in terms of positioning so the application would know which painting, sculpture or object art you were standing in front of. What a fabulous example that would be!

Play and fun are essential for children. That is how they learn. It's the same for adults. Play re-opens neuroplasticity. Adults learn best when they feel safe, curious and engaged.

More than 60% of the people in the US, Canada, the UK and Australia fear AI, according to a global survey of more than 23,000 people by Ipsos. When in a state of fear, adults aren't open to learning. Given that many of the media messages about AI and deepfakes create fear, experiences like those offered in the Dalí Museum can counter this by engaging people and opening minds.

Seligman: Father of Positive Psychology

His AI Digital Twin is designed to help millions of Chinese with depression

Martin Seligman is the founder of positive psychology, the study of human strengths and well-being. Seligman studied positive emotions, character strengths, and what makes life fulfilling. His work was aimed at enhancing well-being. His books, including *Authentic Happiness* and *Flourish*, popularized concepts like optimism and resilience, and has greatly influenced therapy, education, workplace well-being programs, and public policy by promoting evidence-based practices that help individuals and communities thrive.

One of Seligman's graduate students, Dr. Yukun Zhao, along with a team of researchers in Beijing and Wuhan, created an AI Chatbot called *Ask Martin* without Seligman's permission or awareness. In 2023, Zhao's team trained an AI on Seligman's writing, creating a talking chatbot whose answers drew deeply from Seligman's ideas, allowing anyone to

access them. Zhao messaged Martin that he'd created a virtual Seligman.

Seligman eventually decided to embrace the digital twin rather than challenge its existence. But if he'd wanted to shut it down, he'd likely have been unsuccessful. Seligman is American but *Ask Martin* is in China, where US laws have little traction.

In the US Senate Judiciary Committee, a bipartisan group of senators are circulating a draft bill titled the NO FAKES Act that, if passed, would force the makers of AI-generated digital twins to license their use from the original thought leader. The bill would allow individuals to authorize, and profit from, the use of their AI-generated likeness — and bring lawsuits against cases of unauthorized use. But even if the NO FAKES Act passes, it will be largely powerless against the global tide of AI technology.

Ask Martin wasn't built with a profit motive. Zhao built it to help millions of fellow Chinese citizens through an epidemic of anxiety and depression.

Seligman is something of a hero in the world of Chinese psychology. His theories on well-being are embedded in Chinese education policies from kindergarten on. Zhao believes Seligman's popularity will help *Ask Martin* as a mental health AI "coach" stand out in the Chinese market.

Seligman is in his eighties. *Ask Martin* will extend his legacy long after he is dead.

This case study raises some interesting questions. For instance, if you query *Ask Martin,* does the digital twin provide the answer from the 25-year-old Seligman as a PhD student at the University of Pennsylvania or the 83-year-old Seligman in 2025? Or, should the digital twin provide a series of answers showing the evolution of Seligman's thinking over his 60-year career?

100-Fold Cost Decline for Creating an Audio Book

An author can create an audio book for 100 times lower cost than in 1990

My first book came out in 1990. It was called *The 100 Best Companies to Work for in Canada* and it was a national bestseller. As a young journalist and one of the three coauthors, I was very proud of it.

At the time, if I had wanted to turn it into an Audio book, it would have cost more than $10,000 – for the narrator, the studio, editing and mastering. For a high-end audio book production, the cost could have trended as high as $50,000 at the time. Add to that hiring a Hollywood A-lister to read it, and who knows how high the cost could have been.

In 2025, a colleague of mine produced an audio of his 80,000-word book using AI tools for less than $100. Think about how hugely deflationary this new technology is. From $10,000 to $100 – that's a 100-fold cost reduction. This makes an author's work incredibly accessible.

I can stand in front of a green screen and record my likeness in 4K for just five minutes then feed it into AI systems which will learn my voice, visage and hand gestures. Then I can feed it one of my 100,000-word books and create hours of training and development video for 100 times less than it would have cost me in 1990. Will this change learning and education?

With these examples above, I would like to argue that AI is just a tool. How

that tool is used will determine whether we think it's good or bad. Most people in the world will use AI for good. For thought leaders, authors, and speakers it offers incredible opportunities. For teachers and trainers, it offers unprecedented reach for their ideas. But for defending against the bad actors who will use deepfakes for nefarious purposes – for fraud, ransomware, scam – we have to prepare ourselves. So, I will turn back to cybersecurity and how to defend ourselves against bad actors who use deepfakes.

You might wonder why I am discussing cybersecurity when this book focuses on deepfakes. When bad actors gain access to corporate email systems, they can gain insight into corporate relationships, partnerships and launch multiple deepfake attacks against our eco system of business partnerships. So, cybersecurity and defending against deepfakes goes hand-in-hand.

Simple Solutions for Defeating Cybercrime

If the accounts payable clerk in Hong Kong had simply called the CFO in the UK to verify the request, she could have prevented the scam. I don't type credentials into a link I've been sent by email or text. Or discuss my tax account with someone who has called me claiming to be from the tax department. And I don't call an organization back on the number provided in the email and text. I call back on the organization's official number.

Equally important is training every employee in basic cybersecurity hygiene. This includes strong password protection practices, using a password manager, enabling multi-factor authentication (MFA); regular software updates and patching, using reputable antivirus, email and phishing awareness, data backup and recovery; storing backups offline as well as in the cloud; testing recovery periodically; removing unused accounts and permissions and ensuring secure networks, using strong Wi-Fi passwords and modern encryption; and avoiding public Wi-Fi or using a trusted VPN.

Questions:

Do you have a safe word for your family? (Remember, grandparents are particularly susceptible to this kind of scam).

What about every employee in your company?

Has everyone in your firm received cybercrime, phishing, and ransomware training?

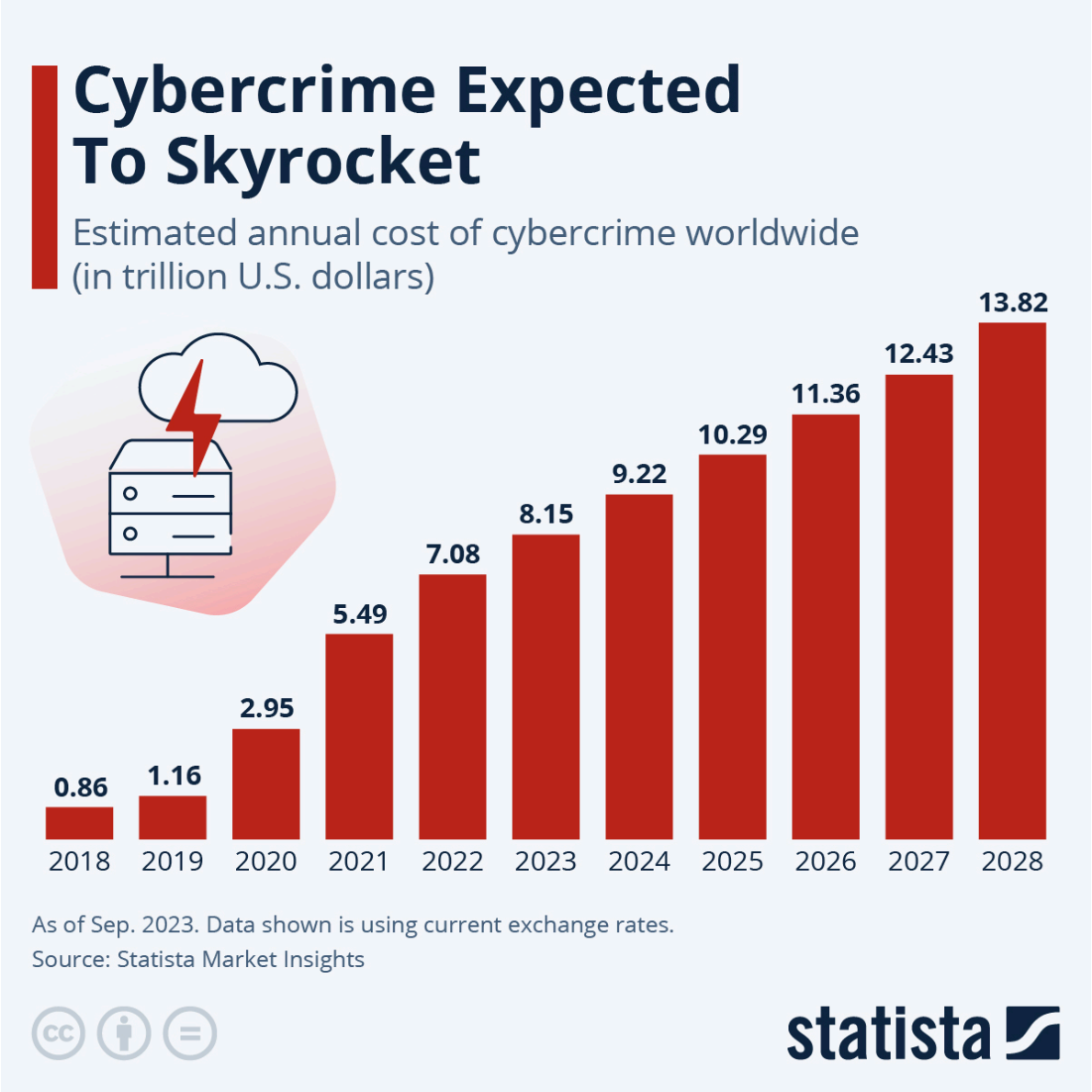
Frightening Cost of Cybercrime

Here are some alarming statistics:

- Cybercrime is predicted to cost $US10.5 trillion globally in 2025, according to the 2025 Official Cybercrime Report from Cybersecurity Ventures. If it were measured as a country, then cybercrime would be the world's third largest economy after the US and China. That's about US$29 billion per day or US$335,000 per second.
- By 2031, cybercrime is predicted to cost the world $1 trillion per month – up from one trillion per year in 2020, according to Cybersecurity Ventures.
- "Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud,

post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, reputational harm, legal costs, and potentially, regulatory fines, plus other factors" said Steve Morgan, founder of Cybersecurity Ventures.

- There are approximately 3.4 billion malicious phishing emails sent every day, according to research from GreatHorn
- Microsoft's Digital Defense Report says its customers alone see about 600 million cyberattacks per day from criminals and nation-states.
- Companies lose $309 million in market value on the day a cyberattack is reported. This peer reviewed study was published in 2025.
- Multiple studies, industry analysis, and experts estimate that only 10% of



Source: Statista, reprinted under creative commons license

cybercrime globally is ever reported to law enforcement or authorities. So official reports and estimates likely only capture one in 10 incidents at best.

Why is this?

a) Organizations fear losing customer trust and investor confidence.

b) The reputational risk damage and negative media publicity can be significantly greater than the financial cost of data breaches or ransomware.

c) Collateral costs (downtime, rebuilding costs, legal, PR, customer churn) are two to three times greater than the cost of ransoms.

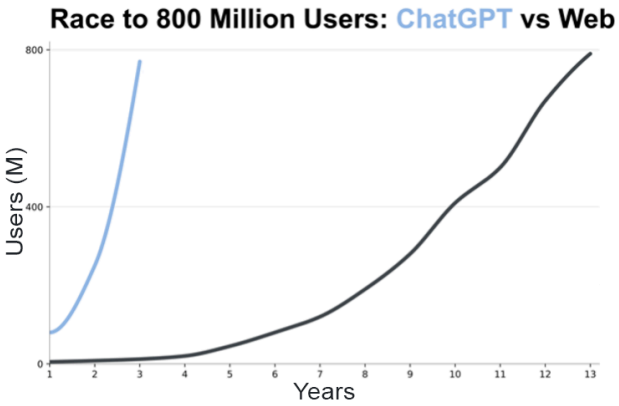
d) Victims assume police or regulators can't or won't do much: attackers are overseas, evidence is complex, and success rates are low.

e) The time, paperwork, and perceived hassles of reporting add huge cost.

- In 2024, the World Economic Forum's Global Risk Report identified "Misinformation and disinformation" as the single biggest global risk through 2026, ahead of extreme weather and interstate conflict.
- A 2024 report by the European Repository of Cyber Incidents analyzing more than 2,506 attack incidents found that 11.9% of the attacks came from China, 11.6% from Russia, 5.3% from Iran; 4.7% from North Korea; 2.6% from Ukraine; 2.3% from the US; 1.8% from Pakistan and 1.7% from Turkey. 13.4% were from other countries and 44.8% couldn't be identified.
- **Smishing** is the use of text messages (SMS, iMessage, WhatsApp, etc.) to trick people into giving up sensitive info (passwords, banking details, one-time codes) or making payments. Recent data suggests that up to 30% of global phishing is now delivered via
- SMS.
- **Vishing** is voice calls that go something like this:
  - "This is your bank / the tax department there's a problem with your account…"
  - "We've detected suspicious activity; read me the code we just texted you…"
    a. "You must pay this fine / fee immediately over the phone…"
    b. "This is FedEx / UPS calling for the brokerage fee to deliver your

Why Corporate Leaders Need to Act Immediately

Bad actors are the fastest to adopt new technology. The rate of technological change we are experiencing is exponential. For instance, it took the web 13 years to be adopted by 800 million users. It's taken ChatGPT less than three



years. The rate of AI adoption is 4.3 times faster than the web's adoption.

When ChatGPT publicly launched on November 30, 2022, it focused on text queries. In 2026, users can create images and video. For images, we have DALL-EE (now embedded in ChatGPT) and Midjourney. For video, we have Sora and Google's VEO 3. As a result, the age of being able to trust what you see at face value is over.

Pet Peeve: Mobile Firms Must Do More

Google reports that it blocks 99.9% of spam, phishing, and malware from reaching its customers' inboxes – billions of messages per day. I really appreciate this. Why then do I get dozens of spam texts and phone calls daily through my mobile network provider? I would think that, if, as a mobile provider, I saw 10 million texts coming from a single IP address to my wireless network subscribers, I might think, "Gee, this might be a bad actor trying to defraud my customers."

Why haven't mobile providers taken a page out of Google's playbook? Mobile users are being defrauded billions of dollars a year globally because mobile companies have not focused sufficiently on this.

Defending Against Cybercrime

The two examples at the start of this chapter are more commonplace than we think. Cybercrime is dramatically underreported for reasons cited previously. When individuals are targeted, they are often deeply embarrassed about falling victim to it. A friend of our family was defrauded of $40,000 by a cryptocurrency scam. She was so embarrassed that she never reported it to authorities.

I was working for two days with the CIOs and CTOs of Canada's largest hyperscalers. One of the firms involved was Palo Alto Networks. One individual had a great analogy: when he began with the firm, he had the notion that he'd go into a bustling nerve center to fight cyberattacks, he imagined going into a room like the underground command center in the movie *War Games* starring Matthew Broderick as David Lightman (a teenage hacker). In the movie, the command center was 150 feet wide, 100 feet deep, with a ceiling soaring 50 feet overhead. The far wall is dominated by a gigantic bank of screens divided into several massive displays: glowing world maps, missile trajectories arcing across continents, digital countdown timers, status grids, and radar-style plots. In front of this are rows of consoles stepping down toward the screens and workstations: CRT monitors and blinking indicator lights on desks — a colossal,

Image from the movie War Games (1983)

functional machine built to manage nuclear war in real time.

But that vision was shattered when he walked into Palo Alto Networks' headquarters and learned that 99.9% of real-time cyberattacks are dealt with by AI and the remainder are dealt with by small group of experts working on their laptops.

Microsoft's Digital Defense Report says its customers alone see about 600 million cyberattacks per day from criminals and nation-states.

AI Isn't New at Fighting Fraud

In 1993, Visa became the first card network to deploy neural-network-based fraud technology at network scale, in partnership with HNC. A neural network is a type of AI. The tech reduced credit card fraud by more than 70% by looking at patterns.

Neural Networks

A neural network is a computer program that identifies patterns. The neural network can't explain why a particular pattern occurs; it only identifies that the pattern exists. Visa has used neural nets to cut fraudulent credit card transactions by up to 90% in some jurisdictions.

A neural network is a program that "learns" by recognizing patterns. If a jewelry shop in Iowa requests authorization for a $5,500 purchase on a client's card, the system looks at their historical pattern of spending and asks, "Has this client ever bought anything in Iowa?" **No.** "Has he ever purchased jewelry?" **No.** Has he ever charged any item for $5,500 to his card? **No.**

If the answer to all three questions is no, the neural net identifies that this requested transaction is outside of the client's normal purchasing pattern, predicts that it's a fraudulent transaction and requests that the store clerk get photo identification. If it's a thief, he/she will run out of the store at this point. If it's the actual client visiting his girlfriend's family for the first time in Iowa and buying an engagement ring to propose, he'll provide the identification and the transaction will go through.

After one seminar, a participant told me that his gas card had been stolen, but that he really didn't worry about it too much. After all, how much gas can a thief steal? At the end of the day, he reported it stolen and discovered that the thief had run up thousands of dollars of charges, going from gas station to gas station buying cartons of cigarettes. Here's a perfect case for a neural network to identify a pattern. Has this customer ever bought a pack of smokes? **No.** Well, then why is he buying thousands of dollars of cartons today all at different gas stations? It's fraud. The gas station credit card provider clearly was not as sophisticated as Visa and hadn't implemented a neural network fraud detection system.

Neural nets can be used to identify overall patterns of behavior in groups of people. In analyzing stolen credit cards, neural nets came to recognize the pattern that thieves use. It takes human ingenuity to find meaning in the pattern, in other words, to understand why the pattern occurs.

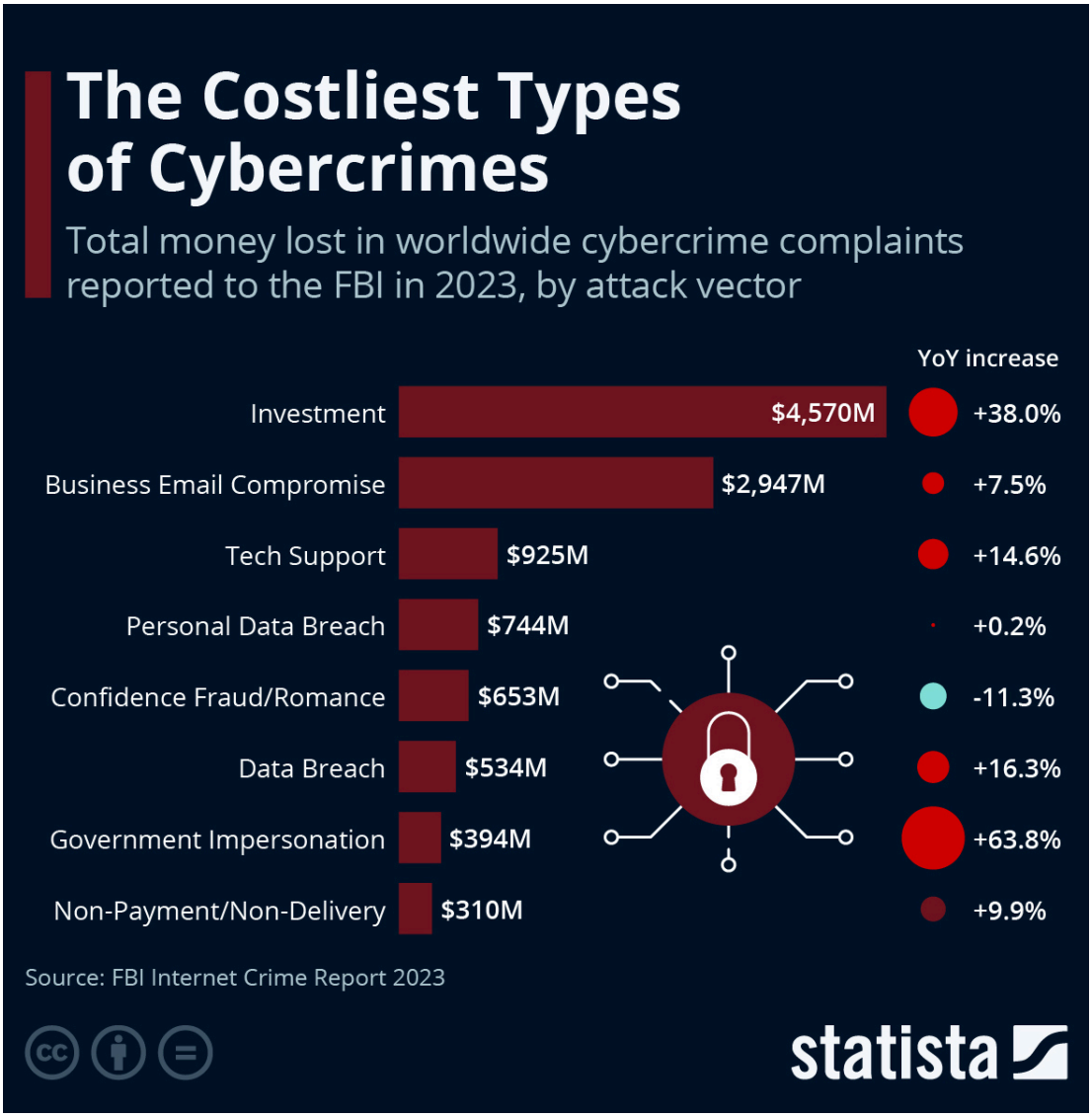
A neural network can help companies better target market their products and services: Car buyers in a certain age group, income bracket and geographical area buy a new car every four years, on average. After individuals in this target group buy a new home and take out a

mortgage, their behavior changes. Over time, a neural net would show that they will buy a new car every eight years as they shift priorities to pay off their mortgage. With this knowledge, a bank could save thousands of dollars in marketing costs by changing its direct marketing programs for car loans from a four-year to an eight-year cycle for new homeowners.

From 2018 to 2028, the annual estimated cost of cybercrime globally will increase 16-fold. Kelly Bradshaw, the former Chief Superintendent of the Royal Canadian Mounted Police (RCMP), notes that only 10% of fraud is reported. And it's not just companies that are at risk; individual Canadians are losing $500 million every year to cyber fraud.

Training

A few years ago, I worked with Canada's largest CEO peer-mentoring network. One of the CEOs had hired a firm to train every employee on cybersecurity. The course highlighted the tricks fraudsters use in phishing and spear phishing



Source: Statista reprinted under creative commons license
Image source: https://www.statista.com/chart/27097/most-expensive-types-of-cyber-crime-us/

schemes and what employees should watch out for. The course was very engaging and successful, receiving high ratings from employees.

Two weeks later, the training firm launched a fake phishing attack. Even after this highly effective training, a staggering 20% of employees keyed in their login details. For me, this highlights three key takeaways:

1) Every employee needs cybercrime, phishing and ransomware training.
2) This training can't be just a one-and-done, but should be an ongoing initiative.
3) It only takes one employee to fall victim to this, and your corporate IT system can be compromised and shut down.

As a leader for your organization, you need to consider the consequences if your company can't operate for weeks or months.

Cyber Insurance

For my firm, we have purchased comprehensive cyber insurance tailored to our business and industry. The insurance company conducted vulnerability testing before offering us a policy and allowed us to mitigate deficiencies to achieve the lowest premiums possible. The insurance covers breaches, legal fees, and ransomware demands, plus the insurance company will help us if we ever do suffer security breaches.

This is a great discipline – to go through vulnerability testing. I recommend it to every organization, hand-in-hand with training.

Why Is This Important Now?

The number and cost of cyber attacks are increasing, and they can have far reaching implications for both organizations and society.

In May 2021, the Colonial Pipeline—which carries nearly 45% of the East Coast's fuel supply across the U.S. — was hit by a major ransomware attack. It became one of the most publicized cybercrimes affecting critical infrastructure. Hackers linked to the DarkSide ransomware-as-a-service group and gained access to Colonial's corporate network through a compromised VPN password lacking multi-factor authentication. Once inside, they deployed ransomware that encrypted systems and stole around 100 GB of data, then demanded payment to restore access.

To contain the breach and prevent further spread, Colonial proactively shut down its pipeline operations, halting fuel flows across thousands of miles of pipeline. This shutdown triggered widespread fuel shortages, panic buying, and price spikes across several U.S. states, prompting a federal state of emergency.

Colonial paid $4.4 million in cryptocurrency to the attackers for a decryption tool, though recovery efforts still relied heavily on internal backups and security work. The pipeline resumed operations after several days, but the incident underscored vulnerabilities in critical infrastructure cybersecurity and led to policy and regulatory responses aimed at strengthening defenses.

Here's another example:

One of the most significant ransomware attacks on a Canadian hospital in recent

years hit The Hospital for Sick Children (SickKids) in Toronto. On December 18, 2022, the hospital's IT systems were compromised by ransomware, which encrypted or disrupted multiple critical internal systems including lab result delivery, imaging systems, phone lines, and medical dictation services.

The impact was immediate: staff had to revert to manual, paper-based processes, leading to delays in diagnostics and operational disruptions. Emergency services and scheduled care continued, but non-critical services saw delays as hospital personnel worked around the outage.

Recovery took weeks. By early January 2023, SickKids had restored 80 % of priority systems, and hospital officials continued working to bring all systems back online.

This incident highlighted the vulnerability of critical healthcare infrastructure to ransomware and the long recovery periods such attacks can impose.

Cybercriminals don't only target large organizations that can pay millions in ransomware. A 2021 report by the Insurance Bureau of Canada (IBC) highlighted that 41% of small businesses that suffered cyberattacks incurred costs of $100,000 and more.

Does this Apply to Every Company and Every Industry?

I was working with a construction company executive team that wasn't really worried about cybercrime and cyber risk. They perceived companies in the digital space like banks and insurance companies, to be more at risk.

In August 2017, MacEwan University in Edmonton, Alberta, fell victim to a sophisticated phishing scam, resulting in the loss of $12 million. The fraudsters impersonated Clark Builders, a construction company working for the university, by sending emails that closely resembled legitimate communications from the vendor. These emails requested changes to banking information, leading university staff to unknowingly transfer $12 million of funds to fraudulent accounts.

As John Chambers, the former CEO of Cisco, used to say, "There are only two types of companies: those that have been hacked and those that don't know they've been hacked." In other words, this means that companies must be eternally vigilant around cybersecurity.

Jim Harris with then Cisco CEO John Chambers at the Consumer Electronics Show, Las Vegas

Industrial Scale Focus on Training and Education Needed

The Future of Jobs Report 2025, released at the World Economic Forum in Davos in January 2025, predicted that 39% of the average worker's skill set will no longer be relevant by 2030. That means that we need an industrial scale focus on learning and development.

Workers need **upskilling** when, for example, 61% of their current skill set is relevant in the future and 39% is not. **Reskilling** is when 100% of their current skill set is irrelevant in the future.

Author Jim Harris with Kevin Weil, CPO of OpenAI

That means that we are entering the era of the most rapid change in human history. While technology advances at an exponential rate, people do not.

The question becomes: "How can we use this new technology to facilitate adoption, accelerate learning and protect our organizations?"

We are actually challenged to reinvent work, to reinvent learning, and to safely reinvent organizations.

I want to turn my attention to learning in this last part of the chapter because learning, training, and development will become critical to future-proofing our organizations.

Here is what I call a meta method: we can use AI to learn how to use AI.

For example, learning how to use AI has revolutionized education. Personalized, AI-driven tutoring and individualized learning consistently deliver significantly better student outcomes than traditional one-size-fits-all methods.

At an AI conference in March 2025, I attended a session with Kevin Weil, Chief Product Officer (CPO) of OpenAI. When asked what excites him most about the future of AI, his answer was clear: personalized tutoring.

Weil cited studies showing that students with a personal tutor will be able to achieve 100 times better learning outcomes than those relying solely on traditional classroom methods. He believes this vision could become reality by 2030.

Weil's optimism is grounded in the rapidly falling cost of OpenAI's models—dropping by a factor of ten every year. In 2025, just two years after ChatGPT entered the public spotlight, the models are not only better, but 100 times cheaper. By the end of 2026, they'll be 1,000 times cheaper than in 2022. This drastic cost reduction is unlocking entirely new applications—ones that were previously financially unfeasible—much sooner than most people realize.

AI is arguably the greatest learning tool in human history. Take Python, the world's most popular programming language. Traditionally, you'd spend anywhere from $3,000 to $15,000 to learn it through a college course or continuing education program. Or, you could open ChatGPT and simply ask: *"What is the first thing I need to learn to start learning Python?"* ChatGPT will teach you—on demand, at your own pace, in real time—for **free**. The impact on using AI to better understand cybersecurity threats can follow this same path for everyone in an organization.

In March 2025, I interviewed Geoffrey Hinton, the 2024 Nobel Laureate often referred to as the "Godfather of AI." I asked him about Weil's vision of AI improving student outcomes a hundredfold by 2030. Hinton thought Weil was overly optimistic, suggesting instead that we could expect a fourfold improvement. The key difference? Hinton was referring to current results, while Weil was envisioning future potential. Either way, the message is clear: personalized AI tutoring can dramatically improve learning outcomes. That's why it's so puzzling that some schools and universities are still banning the use of AI.

Author Jim Harris with Nobel Laureate Geoffrey Hinton

CASE STUDY:

Personalized AI Tutor

The case for AI tutors is compelling. Personalized instruction can adapt to individual learning styles, helping each student learn in the way that works best for them.

Adeel Khan is the founder of Magic School. It's an AI startup with the mission of making teachers' lives easier and improve student outcomes by giving educators powerful, safe AI tools. I met him at Web Summit in Vancouver and interviewed him about his startup's successes.

A teacher in Denver implemented Magic School's tool for improving writing in his class. The teacher uploaded the rubric for that statewide exam (a rubric is the way a student's work is graded). The tool gave students immediate feedback every day on their writing skills, each day focusing on a different part of the rubric. The students achieved a 28% improvement on the statewide test. It's Important to note that the teacher had no special training, and the school board didn't promote this initiative. So, what could be achieved with a concerted, systematic approach?

Adeel himself used to be a teacher. He had 140 students across five periods every day. He pointed out that a single teacher can't give individualized feedback to every

student every day on their writing skills, but an AI can.

"To learn a language, you need to speak it."

English is a mandatory subject in schools across the globe, but teacher shortages persist. Conversational AI tutors designed for children could provide scalable, affordable support—anytime, anywhere. Cybersecurity needs to be addressed

Two Techniques: Stacking & Simplifying

One CEO client of mine shared how his son, a university student, is using **Otter.ai** to transcribe all his lectures. When he encounters something he doesn't understand, he pastes the transcript into ChatGPT and uses prompts like:

- "Explain this to me as though I'm a seven-year-old."
- "Now explain it like I'm twelve."
- "Create a remedial lesson plan with exercises that build from simple to complex to help me understand this concept."

I call this **"stacking"**— taking the output from one AI tool (Otter.ai) and feeding it into another (ChatGPT).

Wordly: Real Time Event Translation

I've been a professional speaker for 35 years. At major high-end conferences, real-time translation was once an expensive luxury. It required three to six interpreter booths, a team of translators, radio receivers, and headsets for attendees—easily costing more than $100,000 for a four-day, six-language event.

Today, organizers can use **Wordly**, an AI-driven platform that takes the conference's audio feed and translates it into over 120 languages. No receivers needed — attendees use their smartphones and earbuds.

But it gets even better. Wordly also provides real-time transcription. I once sat next to a deaf French woman who was reading the speaker's words — in French — on her phone as they were being spoken in English on stage.

So instead of offering just six languages, Wordly offers 120. Instead of costly equipment rentals, everything runs through personal devices. And instead of a $100,000 bill, it can cost as little as $1,500. That's a 98.5% cost reduction—while also making events dramatically more accessible.

In other words, multinational organizations can drive cybersecurity awareness and training in multiple languages.

Consider how using AI tutors for cybersecurity at different levels might work. Individuals can ask AI to look at their individual systems and highlight weaknesses: teams can have AI look at

cross-departmental work processes and workflows and identify missing links and fragilities; organizations can use "stacking" different AIs to take an organizational view.

AI is ushering in the greatest revolution that learning of every kind has ever seen. Using AI to beat AI will be the new norm, creating "good actors" working for security for our benefit will change the face of security.

Summary:

10 Things You Can Do to Protect Your Bottom Line & Reputation

1. Invest in mandatory cybersecurity training for every employee.
2. Ensure onsite and offsite automatic backup procedures to protect your data.
3. Implement multi-factor authentication (MFA).
4. Have your training firm run simulated phishing attacks.
5. Hire an outside firm to perform vulnerability testing.
6. Make sure your IT team regularly updates the software with security patches.
7. Gamify it: reward employees who pass the test with a free firm-branded coffee mug.
8. Have different employees lead the training every quarter. The best way to learn something is to teach it. Stephen Covey, who wrote The 7 Habits of Highly Successful People, used to always promote learners becoming teachers.
9. Get cybersecurity insurance in your company. Our insurance firm gave us lower rates once they conducted penetration testing and cyber readiness testing for our systems.
10. Include cybersecurity training as a mandatory part of onboarding before granting new employees access to IT systems.

TESTIMONIALS

As CEO of Legal Aid BC, I was deepfaked via random phishing emails to a staff of 250 people. Even worse would have been deepfakes from when I was Attorney General, or as the National Director of the Canadian Civil Liberties Association. Deepfakes don't "break" your systems so much as route around them—by borrowing a leader's voice, a colleague's face, and the organization's reflex to comply. Harris makes the point without melodrama, then does the more useful thing: he turns anxiety into controls. The checklist at the end is a sober starting place for any organization that still thinks cyber risk is something the IT team can "handle."

Hon. Michael Bryant, E.C.O.
35th Attorney General of Ontario

Jim Harris connects the dots between deepfakes and the real business risk leaders face right now. What I appreciated most is how practical and grounded this is—clear examples, plain-English explanations, and simple steps any organization can implement immediately. As the founder and CEO of a mid-sized professional services firm, I'm constantly balancing growth with risk management. This work gave me a sharper framework for protecting our people, our clients, and our finances—especially around verification habits, training, and cyber hygiene. It's a timely, actionable wake-up call delivered with optimism about how AI can also be used for good.

Kevin Gauci,
Founder & CEO
(Mid-sized Professional Services Firm)

Drawing on decades of experience, Jim delivers a clear, practical, and highly relevant perspective on deepfakes and cyber risk. He moves beyond headlines and fear-driven narratives to focus on what leaders truly need to understand and do. Through compelling case studies and actionable recommendations, this chapter equips readers to make informed decisions and strengthen their organizations in an increasingly complex digital landscape. Jim's insight, credibility, and balanced approach make this an essential read for today's leaders.

Todd Millar, CEO
TEC Canada

Jim Harris hits the mark by emphasizing that self-regulation is essential in an unregulated digital world. Individuals and corporations must erect their own guardrails against the dangers posed by AI through education, training, and vigilance.

Diane Francis
Editor-at-Large at *The National Post*
& best-selling Substack author

This is an excellent book that will arm you with tactics and techniques to create a personal and professional career loaded with successful outcomes.

Nido R. Qubein,
President High Point University
#1 Best-Run College in the Nation,
as rated by The Princeton Review

***The Age of Fakes!** is a timely, accessible, and sobering look at how AI abuse, fake news, and disinformation are reshaping economies, politics, and our everyday lives. Jim Harris' analysis of deepfakes and cybercrime is especially useful. This is a valuable read for anyone interested in AI and how it's shaping our world.*

Peter Buchanan,
Master Chair TEC Canada & President of
Management Transitions Ltd.

Required reading for anyone in risk, compliance, or audit. What makes it exceptional is how clearly it connects deepfakes to enterprise risk—not as a niche cyber issue, but as a systemic threat to financial controls, reputation, and trust. If

your organization still treats deepfakes as a communications issue rather than a core risk domain, this will change how you think—and how you act.

Irene Vantaaki,
Founder, Davos Lodge,
an invitation-only gathering during the World Economic Forum

Jim Harris has written the chapter every business owner needs right now. What makes it exceptional is Harris' refusal to indulge in fear-mongering while never downplaying the genuine threat. But Jim doesn't leave you paralyzed. He equips you with practical, implementable defenses that actually works.

The chapter's brilliance lies in its accessibility. Jim translates trillion-dollar cybercrime statistics into actionable steps any company can implement immediately. If you're responsible for protecting your company's reputation, assets, or customer trust, this chapter isn't optional reading—it's essential survival instruction for the AI age.

Scott Wilson, CEO, GeekCertified.com
AI Instructor, McMaster University's DeGroote School of Business

---

While all organizations are concerned about how to drive value from AI, this chapter reminds us that with invention and innovation also comes very real risks. This chapter forces us to balance the race for competitive advantage and ingenuity with how to verify decisions and actions. The perspectives and warnings here are immediately applicable to both companies and individuals alike.

Traci Gusher,
AI Executive

What makes this powerful is its realism. Harris acknowledges that regulation will always lag technology, especially across borders. The discussion of underreported cybercrime, jurisdictional limits, and public trust erosion is sobering. The chapter argues for education, resilience, and institutional redesign as the only sustainable response. This is one of the clearest, most grounded explanations of why AI governance must focus on systems and people—not just laws.

This chapter changed how I think about truth. I expected a technical discussion about deepfakes. What I got was a clear-eyed exploration of trust—how it's built, how it's exploited, and how easily it can be broken. Harris connects personal stories, global data, and practical advice in a way that feels urgent but not overwhelming. It will make you more alert, more informed, and better prepared for the world we're already living in.

R "Ray" Wang,
Principal Analyst & Founder,
Constellation Research, Inc.

If you're still treating cybersecurity as "an IT issue," you're already behind. In the age of deepfakes, authority can be forged, urgency can be manufactured, and reality can be spoofed on demand. Jim Harris makes the case that the new perimeter isn't your network—it's your people, your processes, and your reflexes under pressure. The solution isn't fear; it's discipline at scale: verification as culture, training as a system, AI as both threat and shield. This chapter is the playbook for leaders who understand that in an exponential world, the cost of being wrong once can be existential.

Salim Ismail,
Author Exponential Organizations
Founder OpenExO Founding Executive Director, Singularity University

ABOUT
the Author

*Jim Harris is a one of North America's foremost thinkers on **AI**, **disruptive innovation, and cybersecurity.** He is one of the world's leading keynote speakers presenting internationally at more than 50 in-person and virtual conferences and events a year. Association magazine ranked him as one of North America's top ten speakers. Jim also leads strategic planning sessions with executive teams.*

*Jim was named the **Speaker of the Year** in 2024 by the largest CEO peer mentoring organization in Canada. He was selected from among the 500 speakers the organization works with.*

His YouTube video The AI Revolution with Jim Harris 2025 at video https://www.youtube.com/watch?v=zmyTJVWyQJI has broken 3.8+ million views.

Jim has led a strategic planning exercise for the CIOs and CTOs of Canada's largest hyper-scalers (Amazon, Google and Microsoft) and leading IT firms in the security space like Palo Alto Networks for the Canadian Forum for Digital Infrastructure Resilience (CFDIR) for Innovation, Science and Economic Development (ISED) for the Government of Canada at the Canadian Centre for Cybersecurity. He has also worked with CSIS (but don't tell anyone).

Jim has published five books. Blindsided! was released in 80 countries and is a #1 International bestseller. His second book The Learning Paradox was nominated for the national business book award in Canada. And his first book in 1990 was a national bestseller. His clients include many health care authorities, health care professionals, pharmaceutical firms along with American Express, Barclays Bank, IBM, Munich Re, the Top 200 CIOs of India, the UK Cabinet Office, SAP, Swiss Re, Walmart, and Zurich Insurance. Between 1990 and 1996 Jim represented Dr Stephen Covey teaching the 7 Habits of Highly Effective People