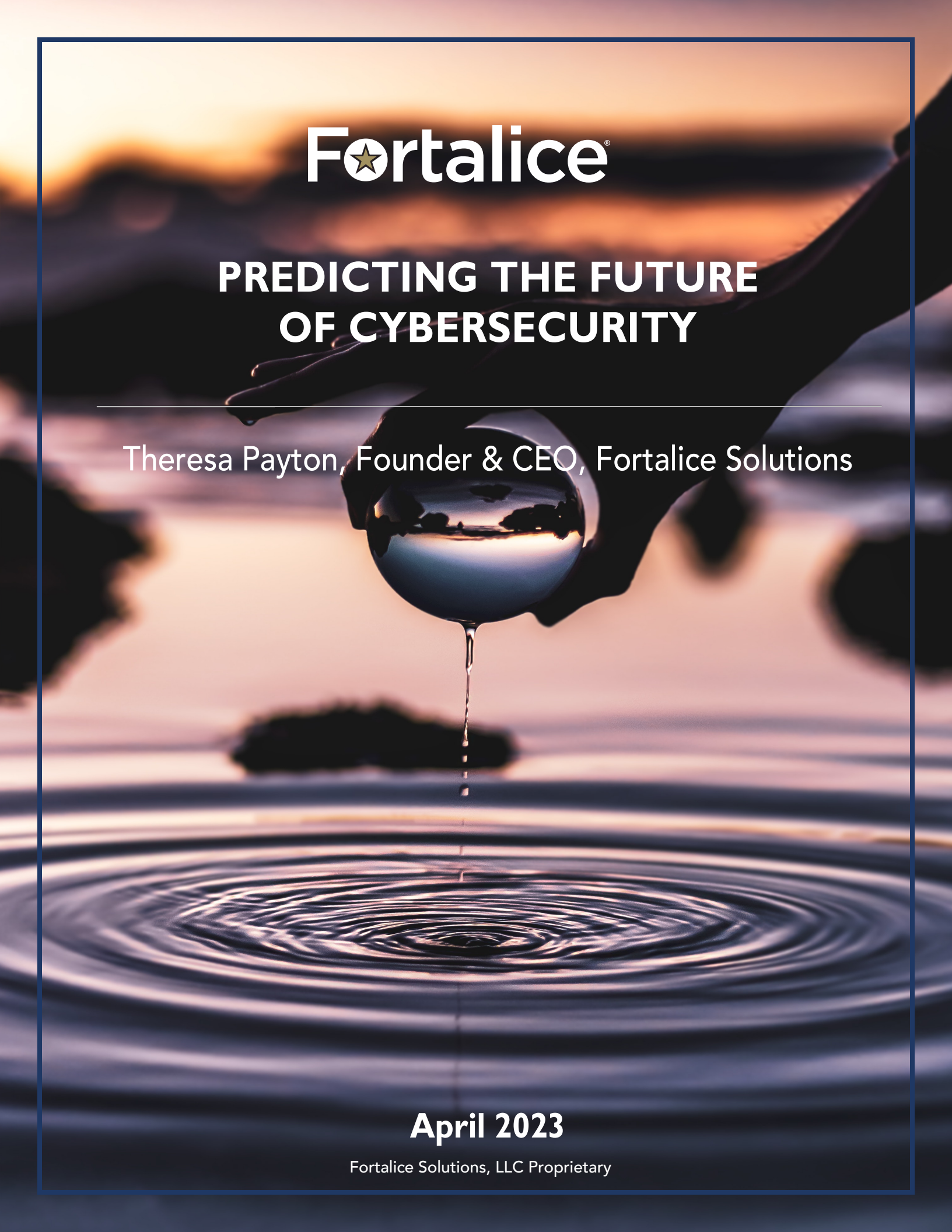


Fortalice®

PREDICTING THE FUTURE OF CYBERSECURITY

Theresa Payton, Founder & CEO, Fortalice Solutions

April 2023

Fortalice

Table of Contents

Cover photo credit: Mark Arron Smith

Fortalice

Introduction

The world of cybersecurity is rapidly evolving, with new threats and malicious actors popping up each year. Try as they might, even the best and brightest cybercrime fighters get caught flat-footed by a new attack vector or malicious code that confounds conventional wisdom. Forget staying a step ahead, oftentimes public and private sector entities are left playing catch up when it comes to protecting their data, their assets, and their people.

Enter, Theresa Payton. Theresa, Founder and CEO of Fortalice Solutions, has been in the cybersecurity prediction business since 2014. Over the years, Theresa has relied on her extensive experience in technology and cybersecurity at the White House and throughout the financial sector to "look into the future," and orient Fortalice towards preparing current and future clients for a range of cybersecurity events.

The Making of a Prediction

Each November, Theresa reviews the latest published cybersecurity research while gathering her own research notes all to foresee how new technological innovations might make their way into the marketplace in the ensuing 24 to 36 months. Her process involves imagining various futuristic scenarios in which these new technologies impact our daily work and personal lives.

> *"I hope my predictions don't come true and you never need them, but my goal with these is to* **engage and empower you and your organization** *to design plans now to combat what is coming next."*
> - Theresa Payton

Additionally, Theresa considers potential criminal activities that could arise as attempts to circumvent safeguards and gain access to valuable data and money. Lastly, she develops predictions on future cybercrime activity by focusing on human user stories. Recognizing that criminals are often experts in human behavior, her goal is to identify their future tactics so individuals and organizations can prepare for, or better yet, prevent potential attacks.

From Prediction to Fruition

Theresa's predictions examine the current cybersecurity landscape and imagine how it will look in two to three years. The decision to make predictions two years out is meant to challenge the standard "one year from now" outlook, and instead truly test her feel and analysis of the trends

within the constantly changing and innovating worlds of cybersecurity and cybercrime. In addition, looking farther out into the future better enables organizations to review her predictions with sufficient time to adjust their strategic roadmaps. Despite the inevitability of dealing with cyber criminals, Theresa finds joy in imagining the positive impacts that technological innovations will have on our future.

Prediction Accuracy and Grading Methodology

Fortalice conducted extensive historic research on the primary topic area for each prediction to measure Theresa's accuracy. Each prediction's final was graded on a scale of 1 to 5 (Cybersecurity Crystal Balls), which was determined based on its accuracy, its relevance within the predicted year or surrounding years, and the impact that it did or did not have on the world.

As you read through the below predictions, you are encouraged to conduct your own research and make an assessment on where Theresa hit, or missed, the mark.

CYBERSECURITY CRYSTAL BALL RATING SCALE

With apologies to the Magic 8 Ball, Theresa's staff has gone through each of her predictions dating back to 2014 and have provided a not entirely scientific "Cybersecurity Crystal Ball" rating.

Fortalice

2014 PREDICTIONS FOR 2016

Prediction #1 — Attacks and Disruptions via the Internet of Things (IoT)

In 2014, Theresa predicted malicious cyber actors would lay waste to tools and electronics made "smart" in the IoT. In 2016,[1] Theresa's prediction proved prescient when the Mirai botnet malware creators launched a series of distributed denial-of-service (DDoS) attacks using IoT devices targeting the domain registration website for Twitter, CNN, and Reddit.

Prediction #2 — Attacks via Outdated Legacy Components

Attackers did not stop with IoT disruptions in 2016. Theresa accurately predicted malicious actors would seek out vulnerabilities in outdated legacy components. This proved prescient in multiple instances, from an $81 million Bangladesh central bank heist[2] to the San Francisco Metropolitan Transit Agency ransomware attack,[3] threat actors made quick work of known vulnerabilities on legacy technology.

Prediction #3 — Supply Chain will be the Weakest Link

By 2016, Theresa believed malicious actors and technological flaws would break the global supply chain, causing major disruptions to the adjacent systems that keep the world running. And although the supply chain was not the primary target, major disruptions to critical infrastructure (e.g., energy,[4] finance[5]) as a weak link proved to cause immense disruptions to other vital international systems.

Prediction #4 — Thumb Drives will Still be an Issue

Despite data storage's move to the cloud, Theresa anticipated disruptions caused by misplaced, broken, or hacked compromised portable storage devices (e.g., thumb drives). To this day, mishandled hardware still causes major data security and cybersecurity events like the time a man who, during a night on the town in 2022[6], lost a thumb drive with an entire city's population data on it. In 2023, it wasn't just malware loaded on a USB. Five Ecuadorian journalists received portable drives in the mail, each designed to explode when activated.[7] Scarily, one did, mildly injuring a TV reporter. A flash drive, indeed.

Fortalice

2015 PREDICTIONS FOR 2017

Prediction #1 — Destructive Break-ins and Deletion of Data via Wiper Malware

In 2015, Theresa accurately predicted that in 2017 malicious cyber actors would turn their attention towards digital break-ins. She correctly called that "wiper malware" – or malicious software that had the ability to totally clear away data – would wreak havoc across the globe, in the form of WannaCry ransomware.[8] Numerous U.S. and international governments and organizations fell prey to WannaCry, which was eventually resolved through critical Windows patching.

Prediction #2 — International Disruption of Business

Continuing the trend of disruptive wiper malware, Theresa correctly predicted further business disruption by wiper attacks via the Petya wiper.[9] The catastrophic distribution of Petya malware was, as dubbed my many reports at the time, "not ransomware, but something far worse."[10] A package that was truly out for destruction, Petya didn't operate with a ransom functionality, and rather was designed purely to wipe clean as many hard drives as possible and make it nearly impossible to restore data.

Prediction #3 — IP Theft on the Rise

In addition to the disruption of business and destruction of data, Theresa predicted that stealing IP would take centerstage in 2017. During that year, there were multiple instances of nation-states, including China, seeking private sector Intellectual Property (IP), both above board (requiring organizations entering China to share their IP) and below board (insider threats from Chinese nationals attempted theft of IBM[11] and SolarWorld IP[12]). This topic was so front-of-mind in 2017 that it became a major talking point in policy and rhetoric from the Trump Administration with its stance on China.

Fortalice

Prediction #4 — Mobile Can't Be the Only 2FA Option

Theresa's prediction for 2017 that mobile two-factor authentication would no longer be sufficient came true, even earlier than she anticipated, in 2016,[13] when NIST published a Digital Authentication Guideline that warned SMS-based 2FA would soon be deprecated. In addition to NIST raising its cybersecurity standard, malicious cyber actors proved the prediction true by taking advantage of the holes in mobile 2FA in 2017[14] to bypass security controls with bank accounts.

Prediction #5 — Backlash Against Lack of Privacy

In 2015, Theresa foresaw public sentiment on privacy (or lack thereof) would lead to a backlash against public and private sector entities and their policies. While a 2017 study noted online shoppers had grown leery of e-commerce companies handling their private information online,[15] the real backlash came a year later when media outlets highlighted gaps in Facebook's privacy protections and the practices of Cambridge Analytica[16] regarding the 2016 U.S. Presidential Election. Despite ongoing privacy violations, only 17 countries, to date, have adopted laws like the European Union's General Data Protection Regulation (GDPR) to protect their citizens' privacy. Notably, the United States does not have a national privacy law.

2016 PREDICTION FOR 2018

Prediction #1 — Wire Transfer Fraud, BEC Will Become Rarely Talked About #1 Crime

In 2018, the business email compromise (BEC) and wire transfer fraud threat vectors had reached a breaking point, just as Theresa predicted. In fact, U.S. intelligence agencies coordinated with counterpart government entities around the world for Operation WireWire[17] to dismantle wire transfer fraud and money mule schemes executed by international cyber criminals. While this operation was a major win for international law enforcement, the frequency of BEC attempts has steadily risen since 2014, remaining an attack surface with a low barrier to entry for malicious actors.

Fortalice

2017 PREDICTIONS FOR **2019**

Prediction #1	Ransomware Moves to "Extortion-ware"

Given the rise of ransomware in the mid-2010s, Theresa predicted ransomware would transition to "extortion-ware" by 2019. While the two tactics are similar, extortion-ware takes the threat next level by demanding payment from victims in exchange for not publicly releasing data (as opposed to ransomware, which threatened to wipe away or lockout data encrypted by malicious code). This prediction came to life in 2019 through the WannaCry[18] and Maze[19] ransomware variations, where actors threatened to publicly reveal embarrassing information of their victims or even turn them into the authorities for made-up tax fraud.

Prediction #2	Deepfake Understanding and Technology will Enter the Conversation

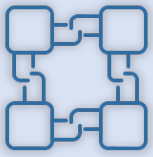
Theresa was two years ahead of the curve on "deepfakes," or the digital alteration of a person's body or face to appear to be someone else (typically for malicious purposes). She accurately predicted deepfake technology would enter the public consciousness and spur a drastic shift in how people interpret and find the truth online.[20] In fact, deepfakes becomes such a commonly used and referenced term in 2019, Facebook and Microsoft teamed up to launch a deepfake video hunting contest.[21]

2018 PREDICTIONS FOR **2020**

Prediction #1	Misinformation Campaign Destroys Company/Industry for Financial Gain

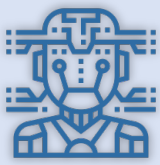
While no one could have imagined the sweeping changes and disruption the world would experience in 2020 from COVID-19, Theresa did predict misinformation would graduate to the next level of global impact. She rightly predicted misinformation campaigns would severely impact companies and industries for financial gain as exemplified by the anti-vax movement, which stirred doubt in the medical profession and pharmaceutical industry,[22] as well as misinformation surrounding politics and the fracking industry.[23]

Prediction #2 — The Blockchain will be Cracked



Eyeing the budding cryptocurrency technology industry, Theresa predicted in 2018 that many crypto advocates would have deemed highly unlikely, if not impossible: a crack in the blockchain. Although 2020 did not bring forward any true cracks in the blockchain, Theresa did accurately anticipate notable deficiencies[24] in its armor,[25] with significant public chatter on how cryptocurrency could face security pitfalls in 2020. In fact, from 2020 to 2022, we saw crypto-hacking levels leap from a $0.5bn impact to $3.8bn,[26] with blockchain bridge hacks on the rise.[27] Finally, in 2022 (two years after the prediction window), Federal law enforcement, investigating the 2016 "Crocodile of Wall Street" $72 million breach of Bitcoin exchange Bitfinex, decrypted a file saved to the suspect's cloud storage account.[28] The file contained more than 2,000 virtual currency addresses and private keys, nearly all of which linked to the hack. Once cracked, authorities ultimately recovered nearly 80 percent of the stolen money.

Prediction #3 — AI-powered Bots Adapt, Evolve to Commit Cybercrimes Without Human Intervention



The evolution of artificial intelligence (AI) has strengthened the efforts of cybercrime fighters and malicious cyber actors, alike. In 2018, Theresa predicted that AI-powered bots would evolve to the point that they were able to commit cybercrimes without a malicious cyber actor pulling the strings. While there have been no major documented cybersecurity events perpetrated by AI bots without human intervention, cybersecurity experts in 2020 did begin asking the question Theresa prompted two years prior about how threat actors could leverage[29] and weaponize AI[30] and amplify their efforts by letting bots do the dirty work.

Prediction #4 — Digital Forensic Anthropology will be a Gig

In 2020, there was some early discussion of developing roles in digital forensics,[31] and more and more colleges around the country offer classes (both undergraduate and graduate-level), certificates, and concentrations in digital forensics. While specific digital forensic anthropology jobs may not yet be flooding sites like Monster and Indeed, if history (and Theresa's prediction track record) is our guide, keep an eye out for Digital Forensic Anthropologist job postings to eventually flood the marketplace given the digital forensic knowledge needed to sort through deepfake forgeries.

Fortalice

2019 PREDICTIONS FOR 2021

Prediction #1 — COVID-19 Innovations will Lead to Advancements in Cybercrimes

In the lead-up to the COVID-19 global pandemic, Theresa knew that cyber criminals would look to capitalize on any major health event and turn technological innovations to their advantage. And while the full extent of COVID-19's impact could not have been predicted, Theresa's prediction was validated by the Verizon Business 2021 Data Breach Investigations Report,[32] which indicated that cybercrime took off in the face of COVID-19 innovations.

Prediction #2 — 5G Technology will Accelerate Cybercrimes

New possibilities of 5G technology for mobile networks led to rampant speculation about its application following its global deployment in 2019. Recognizing malicious cyber actors never sleep, Theresa predicted 5G technology would lead to innovations in cybercrime. Both sides of the cybersecurity battle benefited from 5G advancement in cellular technology, but her prediction for major cybercrime acceleration may have come early. Although 5G likely did impact cybercrime in 2021, most of that year's major mobile network security news involved 5G rollout concerns, specifically its impact on aviation.[33]

Prediction #3 — Misinformation Campaigns will Hit Global Elections

While much of Theresa's prediction ended up starting with the 2020 U.S. elections, the situation carried over into 2021 with prior election fallout and the 2021 elections across the globe. The combination of nation-state actors[34] and readily available social media data[35] has created an election security threat that doesn't appear to be going away anytime soon from fake news in France,[36] to Brexit manipulation in United Kingdom,[37] and to heightened fact-checking and monitoring services across Latin America.[38]

Prediction #4	AI Poisoning Will Come to the Forefront

In 2019, Theresa accurately predicted that in 2021 the growth and manipulation of AI technology would lead to more sophisticated cyber-attacks. Since that time, attacks that poison the "data well"[39] have forced data scientists to rethink their own models[40] and rely on human intervention to counteract malicious actors.

Prediction #5	Ransomware will Go All-in on the Cloud

In 2019, Theresa knew ransomware would play a major role in the future cybersecurity battles of 2021. While 2021 did not feature a major ransomware disruption against a top cloud provider as she predicted, there were still major ransomware events,[41] including the well-publicized attack on Colonial Pipeline,[42] the largest pipeline system for refined oil products in the United States.

2020 PREDICTIONS FOR **2022**

Prediction #1	AI will be the New Peeping Tom

During the COVID-19 pandemic in 2020, Theresa recognized malicious cyber actors would look for new ways to exploit the public while so many people around the globe were quarantining at home. With that in mind, Theresa predicted that threat actors would leverage AI to conduct digital voyeurism as a common practice in 2022. While there may not have been any headline-grabbing instances of AI acting as a "Peeping Tom" in 2022, the increased usage of cameras on our everyday IoT devices[43] as well as the sophistication of surveillance technology makes AI voyeurism[44] a legitimate issue to monitor soon.

Prediction #2	Digital Walk-ins will Leverage Digital IDs

According to the 2021 FiVerity Synthetic Identity Fraud Report,[45] "synthetic identity fraud" accounted for the theft of $20bn in the U.S. payment system in the prior year, validating Theresa's 2022 prediction concerning the abuse of Digital IDs through "digital walk-ins" and stolen identities. This should serve as a cautionary tale for organizations and government entities seeking to leverage digital identification as a tool to decrease fraud.[46] Once malicious cyber actors learn how to leverage and scale digital ID cracking tools,[47] this technology segment will be rife for exploitation.

Prediction #3	Mini-Black Swan Banking Event

Sneaking in under the gun to close out 2022, the FTX black swan banking event shook the cryptocurrency exchange industry and retail/speculative investor sector to its core. The unapologetically bold nature of FTX founder Sam Bankman-Fried[48] coupled with prominent celebrity cryptocurrency endorsements (e.g., glut of 2022 Super Bowl crypto-focused commercials), only further amplified this crypto banking crisis, causing ripple effects across cryptocurrency and the entire financial sector.[49]

Predictions Coming Due

Already in the first few months of 2023, Theresa's predictions from 2021 are beginning to take shape. We will withhold judgment on their final ratings until the end of December 2023.

Prediction #1	Space will be Hacked

In 2021, Theresa predicted that space would become an attractive target for malicious cyber actors in 2023 due to the ongoing race to send private citizens to space and the increased connectivity with Low Earth Orbit (LEO) satellites. First, she believes space will be hacked beginning with the disruption of new connectivity provided by Low Earth Orbit (LEO) satellites. Then, as governments and businesses rush to

"As low-orbit satellites become more integral to humanity's infrastructure, they are going to be targeted by cybercriminals."

connect the disconnected via a string of LEO satellites, these will become a prime target for cybercriminals.

Impacts will ripple out from the LEO satellite disruption, putting critical transportation infrastructure will be at risk, as everything from trucks, autonomous delivery vehicles, planes, shipping vessels, and more are dependent upon GPS, continuous navigation, and communications with timely updates.

Prediction #2 — AI Code Generators will Produce Dormant Security Flaws

As AI-supported software development takes hold and code generators become more popular, Theresa predicts that this combination will provide the next great frontier for third-party supply chain attacks in 2023. By leveraging machine learning to augment developers' processes, the AI generated code should, in theory, be more secure and reliable. However, it only takes one successful social engineering campaign to allow a malicious cyber actor to taint the machine learning or inject a change into the algorithm to generate dormant security flaws they can take advantage of later.

"My concern is there will be dormant security flaws in AI-generated code."

Prediction #3 — Forgeries and Theft Rock the Blockchain

Keeping her eye on the blockchain in 2021, Theresa predicted that in 2023, cybercriminals will harness computing power and AI to find a vulnerability in blockchain hashing. This will allow them to mimic the blockchain to conduct stealth movement to pilfer cryptocurrency, NFTs, and other items stored on the blockchain and replace them with decoys. This will make it appear as if the theft never happened.

"People believe the blockchain is un-hackable, impenetrable. But there are cracks in the armor…and people won't realize it until it's too late."

Fortalice

Looking Into the Future

Theresa's most recent predictions from 2022 paint a grim picture for how malicious cyber actors may leverage AI and smart technology in 2024:

Prediction #1 — "Franken-frauds" and Deepfake AI "Persons" will Enter the Workforce

In 2024, Theresa predicts that the ability to create "Franken-fraud," or synthetic, identities will become automated and run in real-time. These "persons" will use AI and big data analytics to test themselves and ensure they look authentic.

Prediction #2 — A Smart Facility Hacked will go into Lockdown and People will be Locked Inside as Hostages

Theresa predicts as organizations do a better job protecting against and recovering from ransomware incidents, malicious cyber actors will move to another ploy as cryptocurrency prices fall from their meteoric rise. In a disturbing twist in 2024, these cybercriminals will hack into intelligent buildings and lock them down with people inside, demanding a hostage payment to release individuals.

Prediction #3 — AI Bots Terrorize and Become Internet Pirates

Taking AI cybercrime to the next level, Theresa predicts that in 2024, cybercriminal syndicates will develop the capability to create "set it and forget it" bot armies of stealthy digital thieves. Using threat intel feeds, machine learning, and AI algorithms, these syndicates will create automated bots to conduct digital surveillance and gather context about organizations from leadership to systems. Bots will scour cybercrime bulletin boards for attack vectors and assess publicly released vulnerabilities to develop a bespoke arsenal of attacks. This weaponized AI will adapt to any organization's environment to penetrate it and operate in stealth mode. They will be self-learning, contextually aware bots that can morph their activities to mimic an organization's trusted users or technology elements. In other words, they will be the pirates of the internet, seas stealing bounty, hiding the treasures, and maximizing damage.

Fortalice

Acknowledgments

Fortalice Solutions conducted research from several media sources and articles that are relevant to Theresa Payton's predictions through the years. We will continue to compile and publish Theresa's predictions each year, along with the measured results weighed against research from the past, present, and future.

Endnotes

[1] Woolf, N. 2016, October 26. *DDoS attack that disrupted internet was largest of its kind in history, experts say*. The Guardian. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.
[2] Spicer, J, and J. Finkle. 2016, May 6. *Before massive Bangladesh heist, New York Fed feared such cyber-attacks*. Reuters. https://www.reuters.com/article/ctech-us-bangladesh-heist-fed-insight-idCAKCN0XX28F.
[3] Gallagher, S. 2016, November 29. *Muni system hacker hit others by scanning for year-old Java vulnerability*. ARS Technica. https://arstechnica.com/information-technology/2016/11/san-francisco-transit-ransomware-attacker-likely-used-year-old-java-exploit/.
[4] Brook, C. 2016, October 11. *Nuclear Power Plant Disrupted by Cyber Attack*. Threatpost. https://threatpost.com/nuclear-power-plant-disrupted-by-cyber-attack/121216/.
[5] Javers, E. 2016, March 24. *US charges Iranians with cyber-attacks on banks and dam*. CNBC. https://www.cnbc.com/2016/03/24/us-charges-iranians-with-cyber-attacks-on-banks-and-dam.html.
[6] Yeung, J. and Y. Kurihara. 2022, June 24. *Man loses USB flash drive with data on entire city's residents after night out*. CNN. https://www.cnn.com/2022/06/24/asia/japan-amagasaki-usb-data-intl-hnk/index.html.
[7] Harding, Scharon. 2023, March 29. Journalist Plugs in Unknown USB Drive Mailed to Him—It Exploded in his Face. ARS Technica. https://arstechnica.com/gadgets/2023/03/journalist-plugs-in-unknown-usb-drive-mailed-to-him-it-exploded-in-his-face/
[8] Chappell, B. 2017, May 15. *WannaCry Ransomware: What We Know Monday*. NPR. https://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday.
[9] Moscaritolo, A. 2017, June 28. *Petya Ransomware: What You Need to Know*. PCMag. https://www.pcmag.com/news/petya-ransomware-what-you-need-to-know.
[10] Goodin, D. 2017, June 28. *Tuesday's massive ransomware outbreak was, in fact, something much worse*. ARS Technica. https://arstechnica.com/information-technology/2017/06/petya-outbreak-was-a-chaos-sowing-wiper-not-profit-seeking-ransomware
[11] Burgess, C. 2017, May 22. *China's theft of IBM's intellectual property*. CSO Online. https://www.csoonline.com/article/3197751/chinas-theft-of-ibms-intellectual-property.html.
[12] Roselund, C. 2017, October 10. *SolarWorld testifies on Chinese IP theft*. PV Magazine. https://pv-magazine-usa.com/2017/10/10/solarworld-testifies-on-chinese-ip-theft/.
[13] Meyer, D. 2016, July 26. *Time Is Running Out for This Popular Online Security Technique*. Fortune. https://fortune.com/2016/07/26/nist-sms-two-factor/.
[14] Cimpanu, C. 2017, May 5. *Hackers Use Flaws in Telephony Core Protocol to Bypass 2FA on Bank Accounts*. Bleeping Computer. https://www.bleepingcomputer.com/news/security/hackers-use-flaws-in-telephony-core-protocol-to-bypass-2fa-on-bank-accounts/.

[15] Forrest, C. 2017, April 24. *Online shoppers are losing trust in e-commerce, study finds*. TechRepublic. https://www.techrepublic.com/article/online-shoppers-are-losing-trust-in-e-commerce-study-finds/.
[16] Meredith, S. 2018, April 10. *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal*. CNBC. https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.
[17] 2018, June 11. *International Business E-Mail Compromise Takedown*. FBI. https://www.fbi.gov/news/stories/international-bec-takedown-061118.
[18] Abrams, L. 2019, April 10. *New Extortion Email Threatens to Install WannaCry and DDoS Your Network*. Bleeping Computer. https://www.bleepingcomputer.com/news/security/new-extortion-email-threatens-to-install-wannacry-and-ddos-your-network/.
[19] Heller, M. 2019, December 17. *Maze gang outs ransomware victims in shame campaign*. TechTarget. https://www.techtarget.com/searchsecurity/news/252475664/Maze-gang-outs-ransomware-victims-in-shame-campaign.
[20] Taulli, T. 2019, June 15. *Deepfake: What You Need to Know*. Forbes. https://www.forbes.com/sites/tomtaulli/2019/06/15/deepfake-what-you-need-to-know/?sh=174763f8704d.
[21] Culliford, E. 2019, September 5. *Facebook, Microsoft launch contest to detect deepfake videos*. Reuters. https://www.reuters.com/article/us-facebook-microsoft-deepfakes-idUSKCN1VQ2T5.
[22] Wu, K. 2020, December 8. *No, the Pfizer and Moderna vaccine development has not been 'reckless.'*. The New York Times. https://www.nytimes.com/2020/12/08/technology/covid-vaccines-senate-hearing.html.
[23] Gore, D. 2020, June 10. *Misleading Ad Targets Biden on Fossil Fuels, Fracking*. FactCheck.org. https://www.factcheck.org/2020/06/misleading-ad-targets-biden-on-fossil-fuels-fracking/.
[24] Frost, L. 2020, June 19. *Hacker reveals how he cracked a Bitcoin address*. Decrypt. https://decrypt.co/32853/hacker-reveals-how-he-cracked-a-bitcoin-address.
[25] Newman, L. 2020, May 18. *Cryptocurrency Hardware Wallets Can Get Hacked Too*. Wired. https://www.wired.com/story/cryptocurrency-hardware-wallets-can-get-hacked-too/.
[26] Agnihori, C. and H. Bourne. 2023, February 7. *Crypto-hacking reaches an all-time high with cross-chain bridge vulnerabilities accounting for $3.1bn in thefts*. Lexology. https://www.lexology.com/library/detail.aspx?g=9d76af46-f2cb-4f46-aee3-fc4f9fc5db81.
[27] Smith, A. 2023, March 5. *Hackers Plundered $21.41M from DeFi Platforms in February 2022*. The Coin Republic. https://www.thecoinrepublic.com/2023/03/05/hackers-plundered-21-41m-from-defi-platforms-in-february-2022/.
[28] 2022, February 9. *Self-styled "Crocodile of Wall Street" arrested with husband over Bitcoin megaheist*. Naked Security by Sophos. https://nakedsecurity.sophos.com/2022/02/09/self-styled-crocodile-of-wall-street-arrested-with-husband-over-bitcoin-megaheist/
[29] Manky, D. *AI: Beating Bad Actors at Their Own Game*. Security Magazine. https://www.securitymagazine.com/articles/92631-ai-beating-bad-actors-at-their-own-game.
[30] Schwartz, M. 2020, November 20. *The Dark Side of AI: Previewing Criminal Uses*. BankInfoSecurity. https://www.bankinfosecurity.com/blogs/dark-side-ai-police-preview-likely-attacks-p-2971.
[31] Rembert, L. 2020, February 28. *How the Cloud Complicates the Digital Crime Scene*. Infosecurity Magazine. https://www.infosecurity-magazine.com/opinions/cloud-complicates-digital-crime/.
[32] Burbidge, T. 2021, May 13. *Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report*. Verizon. https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report.
[33] Shepardson, D. 2021, December 15. *U.S. airlines warn 5G wireless could wreak havoc with flights*. Reuters. https://www.reuters.com/business/aerospace-defense/us-airlines-warn-5g-wireless-could-cause-havoc-with-flights-2021-12-15/.

[34] 2021, March 17. *Russia's Putin authorised pro-Trump 'influence' campaign, US intelligence says*. BBC News. https://www.bbc.com/news/world-us-canada-56423536.
[35] Bergengruen, V. and B. Perrigo. 2021, March 23. *Facebook Acted Too Late to Tackle Misinformation on 2020 Election, Report Finds*. Time. https://time.com/5949210/facebook-misinformation-2020-election-report/.
[36] Cobert, S. 2022, January 11. *Macron warns against fake news ahead of French election*. AP News. https://apnews.com/article/technology-france-elections-media-paris-79bfebc4556c022ceb6d43ff1eebda60.
[37] Clarendon, M. 2021, February 16. *Fake News in Light of Brexit*. https://www.dgen.org/blog/fake-news-in-light-of-brexit
[38] Rauls, L. 2021, October 19. *How Latin American Governments Are Fighting Fake News*. Americas Quarterly. https://americasquarterly.org/article/how-latin-american-governments-are-fighting-fake-news/.
[39] 2021, October 15. *What is data poisoning, and what is the antidote?* Information Age. https://www.information-age.com/what-is-data-poisoning-what-is-antidote-18874/.
[40] Violino, B. 2021, April 12. *Analytics in the cloud: Key challenges and how to overcome them*. CIO. https://www.cio.com/article/191573/analytics-in-the-cloud-key-challenges-and-how-to-overcome-them.html.
[41] Rundle, J. 2021, December 17. *Cyberattack on Payroll Provider Sets Off Scramble Ahead of Holidays*. The Wall Street Journal. https://www.wsj.com/articles/cyberattack-on-payroll-provider-sets-off-scramble-ahead-of-holidays-11639778286.
[42] Osborne, C. 2021, May 13. *Colonial Pipeline ransomware attack: Everything you need to know*. ZDNet. https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/.
[43] 2022, May 25. *"How Dare They Peep into My Private Life?"*. Human Rights Watch. https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments.
[44] Silver, J. 2022, December 18. *Voyeurism takes disturbing turn as mini cameras become more accessible*. TribLIVE. https://triblive.com/local/regional/voyeurism-takes-disturbing-turn-as-mini-cameras-become-more-accessible/.
[45] 2021, October 11. *FiVerity Introduces 2021 Synthetic Identity Fraud Report*. FiVerity. https://www.fiverity.com/resources/fiverity-introduces-2021-synthetic-identity-fraud-report2.
[46] Belanger, A. 2022, October 31. *Massive pandemic relief fraud has Congress eyeing digital IDs*. ARS Technica. https://arstechnica.com/tech-policy/2022/10/massive-pandemic-relief-fraud-has-congress-eyeing-digital-ids/.
[47] Nash, J. 2022, October 27. *Lesson unlearned: More US kids are being hit by digital ID fraud than last year*. Biometric Update. https://www.biometricupdate.com/202210/lesson-unlearned-more-us-kids-are-being-hit-by-digital-id-fraud-than-last-year.
[48] Egan, M. and A. Morrow. 2022, December 13. *FTX founder indicted on eight criminal charges including fraud and conspiracy*. CNN. https://www.cnn.com/2022/12/13/business/sam-bankman-fried-charges/index.html.
[49] Browne, R. 2022, November 22. *Collapsed crypto exchange FTX has about $1.24 billion of cash in total — but still owes at least $3.1 billion*. CNBC. https://www.cnbc.com/2022/11/22/collapsed-crypto-exchange-ftx-has-about-1point24-billion-of-cash-in-total-but-still-owes-at-least-3point1-billion-.htm

Fortalice