Fortalice

Opening Thoughts

Thank you for the opportunity to speak with you - I loved our time together.
My goal with this document is to supplement my advice to help you thrive with your technology and innovation programs while you bolster privacy and cybersecurity governance efforts in 2023 and beyond.
Best Regards,
Theresa Payton

Assessing the Current Cyber Threat Landscape

Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025

Cybercriminals will come and go. Technology's list of what's-hot and what's-not will change. As we hit mid-2023, there are three core principles for security that I want to share with you. I leveraged these in my work at the White House and they endure today in my consulting practice. These three principles will stand you in good stead no matter what threats you face.

Master Human Nature. Educate yourself about what drives human nature and incorporate that understanding into your cyber security. You need to learn from user stories for your employees and customers.

Know the criminals. Create decoys of fake but authentic-looking human profiles and systems that look valuable and leave the decoys vulnerable to cybercriminals. Then, study the criminal elements that attack the decoys and learn from them.

Beat the criminals at their own game. Leverage the power of Artificial Intelligence (AI) and behavior-based analytics to create behavior-based profiles of employees as well as profiles of criminal activities. Then, use those profiles to create a "digital bodyguard" to protect the good, hard-working humans against digital criminal behavior.

Fortalice

2024 Predictions

To continue to better prepare for the future, I have predictions of how cybercriminals may decide to invest their time and energy in 2024.

Juniper Research reports that the collective cost of data breaches will reach $5 trillion by 2024. They attribute this to the fines levied, such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), and the predicted 70 percent rise in cybercrime between now and 2024.

In 2024, researchers predict:

- More than 50% of Internet traffic inside homes will be from appliances and other home devices.
- Global mobile web traffic equals 84 exabytes
- Global Internet traffic grows to 348 exabytes.
- Wondering how big an exabyte is? A single exabyte is equal to 1 billion gigabytes.
    - As pointed out by the cloud storage company Backblaze, if your average smartphone has about 64 GB of built-in storage, 1 exabyte would be enough data storage for 1.56 million phones.
    - Want more context? Let's go galactic: if 1 gigabyte were the size of the earth, one exabyte would be as big as the sun!

Prediction 1: "Franken-frauds" and Deepfake AI "persons" enter the workforce.

- The ability to create Franken-fraud or synthetic identities becomes automated and is run in real-time using AI and big data analytics to test and ensure it looks authentic.
- The war for talent is real, and remote roles for knowledge workers is an ongoing option. As companies automate their resume scanning processes and conduct remote interviews, fraudsters and scammers will leverage cutting-edge deep fake AI technology to create "clone" workers backed up by synthetic identities. The digital walk into a natural person's identity will be nearly impossible to deter, detect, and recover.
- Design Considerations/Actions:
    - Monitoring: Conduct ongoing monitoring of employee and executive data.
    - In-Person Validation: Review hiring practices to ensure that even remote employees must meet with someone in person to provide proof of identity.
    - No Single Fix: Understand that no product solution can combat this. It will require a commitment to evidence of identity based on data modeling and orchestration.

- Multi-Layered Approach: Ensure multi-layer identity validation using several data sources, digital patterns and signals, verification of documents, and strategic implementation of biometrics.

Prediction 2: A Smart Facility hacked into lockdown and people locked inside as hostages.

- As organizations do a better job protecting against and recovering from ransomware incidents, cybercriminals will move to another ploy as cryptocurrency prices fall from their meteoric rise. They will hack into intelligent buildings and lock them down with people inside, demanding a hostage payment to release individuals.
- Design Considerations/Actions:
  - Architecture: Retain an architecture plan for the Internet of Things (IoT) that ensures the architecture is a "no trust," borrowing from the zero-trust architecture. One example is requiring IoT to authenticate using multifactor authentication. Cordon off each IoT device into a segmented zone of internet access. Connectivity to another IoT device or a system should be tokenized and not in an "always on" state.
  - Asset Inventory & Monitoring: Develop a comprehensive IoT asset inventory and a monitoring plan for each IoT device added to the building. The monitoring plan should provide knowledge of ongoing security, privacy patches, install dates, known vendor issues, persistent digital behavior, collection of log files of the IoT devices, and continuous monitoring of IoT transmissions.
  - Vendor Management: Ask vendors to provide self-certification and, where applicable, third-party certification to comply with the international standards of IEC 62443, ISO 27001, and the European NIS Directive. Leveraging global standards assists your organization in ensuring the implementation of standardized security processes from the vendors.
    - Note: IoT should be treated as a vendor management and supply chain issue and fall under the same guidelines and assessments.
  - Have a Playbook: Maintain Incident Response playbooks that explain how to respond to a compromise or known threat to IoT, covering threats to operational resiliency.

Prediction 3: AI bots terrorize and become internet pirates.

- Cybercriminal syndicates will develop the capability to create a "set it and forget it" bot army of stealthy digital thieves. Using threat intel feeds, machine learning, and AI algorithms, cybercrime syndicates create automated bots that can conduct digital

surveillance and gather context about organizations from executive leadership to networks and systems.

- The bots will scour cybercrime bulletin boards for attack vectors and assess publicly released vulnerabilities to develop a bespoke arsenal of attacks. Weaponized AI can adapt to any organization's environment to penetrate it and operate in stealth mode.
- The bots will be self-learning and contextually aware, able to morph their activities to mimic an organization's trusted users or technology elements. They will genuinely be the pirates of the internet seas, stealing bounty, hiding their treasures, and maximizing damage.
- Design Considerations/Actions:
    - Assume Breach: Implement micro-segmentation of everything; tokenize authentication and access; implement continuous monitoring of data flows, machine activity, and user access points. Make what they take worthless by enforcing the highest standards for the encryption of data.
    - Deploy AI Pirate Hunters: Create your own AI pirate hunters to alert your technology teams to suspicious and anomalous behavior. This AI Pirate Hunter can inspect enterprise devices, user logins, network traffic, and more.
    - Design AI for Autonomous Response: Leverage your existing incident response playbooks and ask what AI can do to mitigate an in-progress attack.

Need more background on these topics? Take a look at the “Background Information” section in this handout’s Appendix!

Other Enduring Principles to Discuss with Your Technology Providers

- Next 30 Days: Collect the top 3 “human-centered design” stories. Model futuristic scenarios & practice playbooks.
- 90-180+ Days: “Segment To Save It”
    - Store backups out of band and encrypted.
    - Prevent Business Email Compromise / Wire Transfer Fraud by implementing a domain name that’s not your public facing domain name, create credentials only used for money movement, talk to your bank about options, create a wire transfer template, consider each person has a code name not easily guessed.

        - Emails on social media, e.g., LinkedIn, are not tied to money movement or sensitive data or processes
    - Single Purpose Identity / Access Controls help combat data and IP theft
- Need a guide? Books on internet safety, privacy, and manipulation campaigns:
    - Protecting Your Internet Identity: Are You Naked Online?
    - Privacy in the Age of Big Data – Brand new 2nd edition
    - Manipulated: Inside the Cyber War to Distort the Truth

With those principles in mind, here are my secured digital transformation and national security takes for 2023-2024, including what businesses needed to know to defeat cyber threat actors this year. My goal is to engage and empower you to design plans now to combat what is coming next.

Global Alerts for 2023-2024

Prepare for the Expected and the Unexpected

"To give you a sense of what we're up against: If each one of the FBI's cyber agents and intel analysts focused exclusively on the China threat – on nothing but China – Chinese hackers would still outnumber FBI cyber personnel by at least 50 to 1." – FBI Director Christopher Wray, Testimony to the House Appropriations Committee's subcommittee on Commerce, Justice, Science, and Related Agencies, April 2023.

Supply Chain Concerns

The Summer of Ransomware and Impacts on Our Supply Chain

"…We're investigating over 100 different ransomware variants, each with scores of victims, as well as a host of other novel threats posed by both cybercriminals and nation-state actors—in addition to China, countries like Russia, Iran, and North Korea. And it's getting more and more challenging to discern where the nation-state threat ends and the cybercriminal threat begins."

-- FBI Directory Wray in his April 2023 testimony.

Fortalice

Russia

Russia's arsenal includes distributed denial of service attacks, misinformation campaigns, cyber assaults on banks and businesses, and even critical infrastructure targeting. Recent incidents, such as the attacks on US airport websites and healthcare organizations, serve as stark reminders of the Kremlin's cyber capabilities.

The Intelligence Community 2023 Report emphasizes Russia's relentless pursuit of military space capabilities and the development of disruptive counterspace weapons. Their comprehensive agenda encompasses jamming, cyberspace operations, directed energy weapons, and ground-based ASAT capabilities.

Notably, a Microsoft report by Clint Watts, GM of the Digital Threat Analysis Center reveals Russia's intensified cyber onslaught against Ukrainian organizations, employing new wiper families and ransomware variants. Their espionage activities have expanded to government agencies across European nations, accompanied by sophisticated influence operations. Boundaries hold no sway over Russian cyber threat actors, as government and defense-related organizations in both Central and Eastern Europe and the Americas face intrusion attempts linked to their intelligence services.

In the face of these multifaceted challenges, fortifying cyber defenses, fostering intelligence collaboration, and nurturing resilience are imperative. Only through a unified and proactive approach can we safeguard our collective security and protect our cherished values.

North Korea

2023-2024 North Korean hacking groups continue to target staff that work in foreign trade, finance, R&D, as well as diplomats and prominent executives. Recent massive database breaches feed their tool of choice which is "credential harvesting". Stealing from password dumps and using tools to generate passwords based on past passwords. One group that's skilled at this is the TA406 group which has targeted individuals far and wide including in the United States, Russia, China, and South Korea. Besides committing economic espionage, they dabble in ransomware and look for ways to steal cryptocurrency. The FBI reported that the Lazarus Group, which is linked to North Korea, attacked the cryptocurrency bridge, Horizon in 2022. They managed to steal approximately $100 million (USD) worth of cryptocurrencies from the bridge transactions. They got off to a fast start in 2023 attacking a cryptocurrency anonymity system called Railgun. They used this hack to launder some of the proceeds from the 2022 Horizon breach.

In April 2023, alleged North Korean hackers infiltrated 3CX, a software firm. The breach, discovered March 2023, provides North Korea with a potential foothold into a broad range of multinational firms, from hotel chains to health care providers that use 3CX’s software for voice

and video calls. The number of companies affected by the hack, and what the hackers did with access to victim networks, remains unclear. However, it is the latest evidence of North Korean hackers' attempts to break into organizations to steal or spy on them in support of dictator Kim Jong Un's strategic interests. Charles Carmakal, CTO at Mandiant Consulting, which 3CX hired to investigate the hack, said the hack shows "an increased level of cyber offensive capability by North Korean operatives". Mandiant said the hackers infiltrated the company's software production environment by first compromising software made by another firm, Trading Technologies. A 3CX employee downloaded the Trading Technologies software that the hackers had tampered with, according to Mandiant. Mandiant said it was the first time it had found concrete evidence of a supply chain attack leading to another supply chain attack.

China

Caught flying spy balloons over the US, 2023 is a year in which their operatives will continue both covert and brazen probes of the US infrastructure. Microsoft revealed in September 2023 that China used generative AI (eg., ChatGPT) to create convincing misinformation and disinformation campaigns targeting U.S. voters in an attempt to influence the Presidential elections. They are focused on political and economic espionage, to include the theft of US R&D. The Washington Post did an investigation into China's government operations and found China had government contracts and projects that included "orders for software designed to collect data on foreign targets from sources such as Twitter, Facebook, and other Western social media."[1] China will continue to implement its Belt and Road Initiative. Supply chain issues will be exacerbated when China invades Taiwan. As FBI Directory Wray said in April 2023 testimony, "…if each one of the FBI's cyber agents and intel analysts focused exclusively on the China threat, Chinese hackers would still outnumber FBI Cyber personnel by at least 50 to 1." From the Intelligence Community 2023 Report Published by the Office of the Director of National Intelligence: *"China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks. China's cyber pursuits and its industry's export of related technologies increase the threats of aggressive cyber operations against the U.S. homeland, suppression of the free flow of information in cyberspace—such as U.S. web content—that Beijing views as threatening to the CCP's hold on power, and the expansion of technology-driven authoritarianism globally."*

[1] The Washington Post. https://www.washingtonpost.com/national-security/china-harvests-masses-ofdata-on-western-targets-documentsshow/2021/12/31/3981ce9c-538e-11ec-8927c396fa861a71_story.html

Fortalice

Iran

When the earthquakes destroyed parts of Turkey and Syria, Iran took full advantage of the disruption to flex their agenda. Political espionage to advance Iran's interests will continue as well as attacks for financial gain. Iran continues to evolve their tradecraft including dabbling in ransomware tools as well as siding with Russia to attack infrastructure. Anyone perceived to mock their regime is a target. February 2023, Microsoft revealed that Iranian affiliated operatives attacked, stole and dumped on the internet the customer data of the French satirical magazine Charlie Hebdo. As I wrote in my book, Manipulated, Iran has large ambitions to influence other through misinformation/disinformation and manipulation campaigns. Microsoft recently released researched indicating that Iran's state-backed hackers and the Iranian government was behind 24 "cyber-enabled influence operations" in 2022, including 17 since mid-June, marking an escalation in Iran's adversarial cyber interests. Microsoft noted that Iran has historically relied on more traditional disruptive hacks, with Russia and China being the only two US adversaries that have previously employed disinformation campaigns in their schemes. From the Intelligence Community 2023 Report Published by the Office of the Director of National Intelligence: *"Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data."*

A Cybercrime Treaty?

Will 2023-2024 be the year of the International Accord on Cybercrime? Perhaps, but likely not.

There is a draft that started in December 2019. Just before the pandemic hit, the U.N. General Assembly adopted a resolution to draft a global comprehensive cybercrime treaty. Prior to the Omicron/COVID19 pandemic, discussions were planned for January of 2022.

The U.N., the U.S., Canada, the EU, and other parties to the Budapest Convention feel this is not the right direction and want to enhance the Budapest Convention treaty on cybercrime.

In early 2023, The Abraham Accords (Israel, UAE, Bahrain, Morocco, Sudan) expanded to include cybersecurity collaboration. See https://www.state.gov/the-abrahamaccords/ for more information on the accords.

Fortalice

Big Concern

Whether it's the extension of the Budapest convention or something new, agreement on the treatment of cybercrime is too vague and not enough work has been done around human rights. We can't even agree globally yet on what constitutes cybercrime. We don't have a framework across all borders regarding how law enforcement needs to work in a cross-border crime and investigation.

Three Steps to Avoid Check Washing and Mail Fraud

If you are mailing checks, consider going inside your post office and using the drop box that's inside and secure.

Check washing is growing in prominence. Here are steps you can take to avoid becoming the next victim.

1. **Exquisite Security Checks**: Indulge in checks adorned with ingenious security features, crafted to bewilder even the craftiest of fraudsters. Ask your bank if they offer these options: chemically sensitive paper, captivating watermarks, and alluring heat-sensitive ink. These features make checks nearly impossible to alter.
2. **Gel Pen Mastery**: Embrace gel ink pens for indelible elegance. These pens are the most resistant to erasure or manipulation.
3. **Vigilant Vigilance**: Keep a watchful eye over your accounts, vigilant for any audacious intrusions or unauthorized withdrawals. Consider using bank features such as positive pay.

5 Steps to Become Unhackable in 15 Minutes or Less

1. Immediately **change all passwords** on all online accounts if they have been breached, or if they have poor passwords (e.g., names of family members or pets, hobbies). Use phrases rather than words.
2. Implement **Multi-Factor Authentication (MFA) on all online accounts**, including personal accounts, which are a bigger target for cyber-criminals.
3. **De-activate any dormant and inactive online accounts**. Even if no longer in use, these accounts still provide an important target for cyber-criminals.
4. Undertake a **digital footprint assessment** to understand the full extent of what information is out there about you.
5. Consider **single use domains and single use emails** for critical access points.

Fortalice

Favorite Tools to Consider

Password Management

- 1Password: 1Password.com
- Leakpeak: https://leakpeek.com/
- Have I been Pwnd?: https://haveibeenpwned.com/
- YubiKeys by Yubico: https://www.yubico.com/

Family Tracking

- Life360: www.life360.com
- Disney's Meet Circle: https://meetcircle.com/

Burner Numbers/Emails

- Google Voice: https://voice.google.com
- ProtonMail: https://proton.me/

Scan Links and Attachments:

- VirusTotal: https://www.virustotal.com/

Have A Web Page or a Mobile App?

There are hidden security & privacy dangers that you need to be aware of.

- Fortalice has reviewed more than 40 companies, across various industries on a pressing cybersecurity topic: internet trackers. This is an issue that has resulted in a class action lawsuit for ESPN and HBO, as well as class actions brought against health care organizations. Based upon our research, this problem is vast and could hit *any* organization that is doing 3rd party marketing and/or customer "listening" to ensure their web experiences are stellar.
- If you have a website or mobile app, you likely have a hidden problem. Multiple organizations' third-party marketing campaign tools are sending their clients' data (e.g., PCI, PII, HIPAA, cell phones, email addresses, IP addresses) from their company websites to social media companies and big tech platforms behind the scenes (e.g., Google Ads, Meta Pixel, HotJar).

To ensure trackers are providing valuable information without disclosing sensitive data, consider the following steps:

- Discover where trackers are deployed. Using our proprietary tool, we have identified some situations in which a tracker, or code related to tracking functions, has been deployed on web pages unexpectedly.
- Develop a process for vetting and approving the use of tracking and similar technology, including IT Security and Legal in the discussion.
- When installing and configuring tracking technology, run tests that emulate common website activities, and ensure only data appropriate for the task is collected and transmitted. We created a fictitious company and deploy various trackers and look for the security and privacy configuration flaws in them and test out approaches to remediate. Consider this practical approach before you install trackers on your site.
- Ensure your Privacy Policy clearly explains the use of tracking technology, and where required, provide a means for users to "opt-out" of tracking.

The Next Steps with Generative AI

In the realm of AI, a captivating future awaits. The projected market value of nearly $1.6 trillion by 2030 showcases its pervasive influence. However, as a dual-use technology, AI poses significant disruptions that cannot be overlooked. To instill trust, organizations must prioritize ethical governance frameworks. While guidance like the OECD Council Recommendation on AI and the EU's Artificial Intelligence Act exist, actionable measures for responsible AI are still lacking. We must learn from past mistakes and transition from policy to practice, implementing clear programs for effective AI governance.

We clearly got a lot wrong when it came to social media. We cannot afford to repeat historical mistakes. To move from policy to practice, organizations should implement clear and structured programs that guide the implementation of AI governance frameworks.

These programs must:

- clearly define the purpose of the AI;
- identify and train the right algorithm and use guard rails to ensure that training data is pristine and engineering biases are counterbalanced;
- and, consider human-centered designs and interaction during the decision-making process.

As AI transcends industries and geographies, the development and implementation of trustworthy AI require collaboration amongst researchers, developers, businesses, and policymakers, ensuring that AI systems align with social values and promote the public good. See our Client Advisory on Generative AI for more information and a draft employee usage policy for consideration: https://www.fortalicesolutions.com/posts/chatgptfuture

Fortalice

Appendix A: Background Information

Synthetic Fraud:

- One of the most pervasive and fastest-growing types of identity fraud is known as synthetic identity fraud. In fact, in the USA, it is the largest form of ID fraud. 2020 losses via synthetic identity fraud was more than $20 billion (Source: Forbes, https://www.forbes.com/sites/forbestechcouncil/2022/08/19/howbusinesses-can-fight-the-growing-threat-of-synthetic-identityfraud/?sh=6093643c2887).
- This is a company problem, not just a consumer problem.

Smart Buildings:

- Smart buildings require an architecture of interconnected Internet of Things, or IoT, devices. The intricate patchwork of devices can range from door access controls to thermostats based upon building occupancy, motion-sensor lighting, and other climate controls, and more. The IoT in a building could also be managed by machines and applications meaning communications are machineto-machine without human intervention.
- According to Palo Alto, 57% of today's Internet of Thing devices are deemed vulnerable to medium or high-severity attacks. (Source: https://unit42.paloaltonetworks.com/iot-threat-report-2020/#:~:text=57%25%20of%20IoT%20devices%20are,attempt%20to%20exploit%20known%20weaknesses.)

AI Use by Cybercriminals:

- Europol predicts that criminals will be able to use AI to sift through company targets and effectively locate and exploit their vulnerabilities.

Appendix B: Resources

Have a Question?
www.FortaliceSolutions.com
Email: Watchmen@FortaliceSolutions.com
Call: (877) 487-8160

Fortalice

For more information on how to protect privacy and secure data when you design social media and web marketing campaigns or customer listening,
https://www.fortalicesolutions.com/posts/consumerprivacy

In the USA, consider contacting the FBI InfraGard to discuss membership for free briefings and information sharing. https://www.infragard.org/
Cybercrime alerts: https://www.ic3.gov/Home/IndustryAlerts
Access to FBI alerts and free tools and resources:
https://www.fbi.gov/investigate/cyber
FBI update on BEC scams: https://www.fbi.gov/scams-and-safety/common-scams-andcrimes/businessemail-compromise

The EU Cyber Direct Site Articulates the Singular and Joint Efforts for cybersecurity across the EU, Canada, UK, Australia, and the USA: https://eucyberdirect.eu/about

The Centro Nacional de Ciberseguranca Portugal (CNCS) provides fabulous resources at:
https://www.cncs.gov.pt/en/

In Canada, you can report cybercrime and fraud and access resources at:
https://www.rcmpgrc.gc.ca/en/new-cybercrime-and-fraudreporting-system
The Government of Canada has fabulous cybercrime prevention resources posted at "Get Cyber Safe": https://www.getcybersafe.gc.ca/en
Canada has a self-assessment tool and resources to assist with setting privacy approaches and strategies published by the Office of the Privacy Commissioner of Canada (OPC). The tool aides medium and large organizations through setting good privacy governance and management.
https://www.priv.gc.ca/en/privacytopics/privacy-laws-in-canada/the-personalinformation-protection-and-electronicdocuments-act-pipeda/pipeda-compliancehelp/pipeda-compliance-and-trainingtools/pipeda_sa_tool_200807/

Ransomware Victim Organization No More Ransom (free removal tools and resources):
https://www.nomoreransom.org/en/index.html

Europol Ransomware Assistance:
https://www.europol.europa.eu/activitiesservices/publicawareness-and-prevention-guides/no-more-ransom-do-you-need-helpunlocking-yourdigital-life