Opening Thoughts

Thank you for having me here today - 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 embark on 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.

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 to 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.
    - Still 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: 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 national security takes for 2023, 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

Prepare for the Expected and the Unexpected

Supply Chain Concerns

Log4j and the Supply Chain

The Log4j vulnerability that hit the news cycle in December 2021 is the most current example of rampant supply chain issues. I expect that 2023 will see continued attacks from cyber operatives in Russia and North Korea. They will take advantage of supply chain vulnerabilities like Log4j or last year's Kaseya or SolarWinds. Their goal will be to leverage a trusted third-party product to allow them inside access and to quietly, in stealth mode, build a pervasive foothold.

Regarding whether Log4j is fixed as of writing this post, the answer is not simple. The solution relies on good old fashioned detective work to find the problematic systems and patch them. We know that big names such as Apple, Amazon, Tesla, and even Microsoft's Minecraft and LinkedIn were impacted. NSA Director Rob Joyce has said that even the tool they use to reverse engineer cyberattacks, (GHIDRA), had to be patched. This issue cannot be fixed by a security team alone; it's the technology teams, such as product development and support, which are often outsourced.

Cybercrime is global and operatives live and work in almost every country that has internet access. Some of the biggest cyber threats for America's national security come from individuals operating within Russia, China, North Korea, and Iran.

Russia

I predicted end of 2021 that Russian would eventually invade Ukraine and that the US will have to respond along with NATO. It's very likely that Putin will decide to continue to leverage cyber tools because they are less obvious. As early as March 2022, I predicted that this may include distributed denial of service attacks, misinformation operations, cyberattacks on banks and businesses within the Ukraine, and attacks on critical infrastructure. On October 10, 2022, Russia attacked US airport websites with distributed denial of service attacks. Late January – Early February Russia attacked U.S. healthcare organizations.

North Korea

In 2023 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 are 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.

China

Caught flying spy balloons over the US, this is a year operatives will continue both covert and brazen probes of the US infrastructure. 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 their Belt and Road Initiative. Supply chain issues will be exacerbated if and when China invades Taiwan.

---

[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

Iran

With the recent earthquakes destroying parts of Turkey and Syria, Iran will take 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.

A Cybercrime Treaty?

Will 2023 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.

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.

Fortalice

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.

Favorite Tools to Consider

Password Management

- 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
- Talkatone: https://www.talkatone.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 been working with multiple organizations across various industries and the law firms that represent them 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.
- Recently, we've seen that 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. 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.
- 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 Promise of Innovation and Web 3.0 Tech

There are endless possibilities if we implement Web 3.0 technologies, for example blockchain and cryptocurrency, correctly! Web 3.0 could provide access to customers of every demographic; the creation of new types of frameworks for liquidity and capital through tokenization of current, traditional assets; and new back-office optimization through extended reality meetings, smart contracts, micro payments, trusted clearing, and more.

Three Foundation Elements

- Have a strategic plan and roadmap.
- Decide the model for Web 3.0 program management: in-house, outsourced, or hybrid.

- Risk Tolerance and Risk Governance: With the evolving regulations, have playbooks in place to support risk, resiliency, handling of cyber incidents, and responding to OFAC/KYC/AML inquiries.

Organization and Personal Segmentation of Cryptocurrency is Key

If you or your suppliers use cryptocurrency, take heed. We recently hit a new milestone: Cybercriminals stole approximately $700 million worth of assets from crypto platforms in the first quarter of 2022! Identity fraud and cryptocurrency scams are real and happening!

What Can You Do?

1. Consider newly issued domain names that are not public facing and single purpose credentials for cryptocurrency assets.
2. Teach everyone that has or interacts with cryptocurrency the latest social engineering schemes.
3. Leverage Multifactor authentication at every point feasible and establish governance and monitoring of authorizations.
4. Assume you will be a victim - Have an incident response playbook for stolen cryptocurrency that you rehearse annually.
5. Various NFT and cryptocurrency asset ownership norms may change. For example, when someone buys an NFT, storing photos or videos in the blockchain is often not feasible due to their size. Many platforms sell you the NFT image and give you a protocol that points to the image. The smart contract is on the blockchain the image might be off the blockchain. Various NFT marketplaces have inherited the vulnerabilities of Web2.
6. Blockchain bridges are a rising threat - Different blockchains have different coins, like countries and currencies. If you want to buy something on a platform that only accepts Bitcoin and you have Ethereum, you must exchange it. This is often OFF the blockchain. A currency exchange of sorts.
7. Hot vs. Cold Storage: The ongoing bane of many security teams is Key management – You may want to consider cold storage which is often hardwarebased wallets (e.g., Trezor, Ledger, or Lattice1). Cold storage usually are USB devices that can be used to generate and store the items and is a layer of prevention for. Your private keys. An attacker may get to your computer but cannot easily jump to get to the cold storage.
8. A best practice emerging is the use of multi-sigs – exactly as it sounds, more than one sign off on the transaction.

A Problem for Everyone: SIM Swapping

Of grave concern to your operations are the growing SIM-Swapping Attacks. The FBI has issued warnings on working victim cases that thieves used a workaround to MultiFactor Authentication.

(For FBI info see https://www.ic3.gov/Media/Y2022/PSA220208).

In fact, the Federal Bureau of Investigation received more than 1,600 SIM-swap complaints in 2021 and estimated losses could tally as much as $68 million. For comparison purposes, losses were $12 million in 2019. Cyber thieves are targeting both crypto and traditional bank accounts.

How Do They Do It?

1. Trick mobile network call centers by posing as you.
2. Send a social engineering phishing attack to your text or email.
3. Insider threats. (E.g., T-Mobile caught an employee taking bribes to do SIM Swapping.)

What Can You Do?

1. For authentication to key organization platforms, consider more than just mobile based messages for authentication protocols. Example: use an app that requires device integrity matching versus an authentication code or message sent via an SMS or text message.
2. For cryptocurrency holders, do not post about your preferred crypto platforms.
3. Consider handing out a "burner" number instead of your actual cell phone number.

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

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/

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

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

Fortalice

"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

CDW Paper on Ransomware: https://www.cdw.com/content/cdw/en/articles/digitalworkspace/are-you-prepared-forthelatest-ransomware-tactics.html

Avast's Free Decryption tools: https://www.avast.com/en-us/ransomware-decryptiontools

Trend Micro Decryption Tools: https://success.trendmicro.com/solution/1114221downloadingand-using-the-trend-micro-ransomware-file-decryptor

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