The U.S. National Cybersecurity Strategy

Lessons Learned and the Path Forward

Matt Cronin

Chief Investigative Counsel

China Select Committee

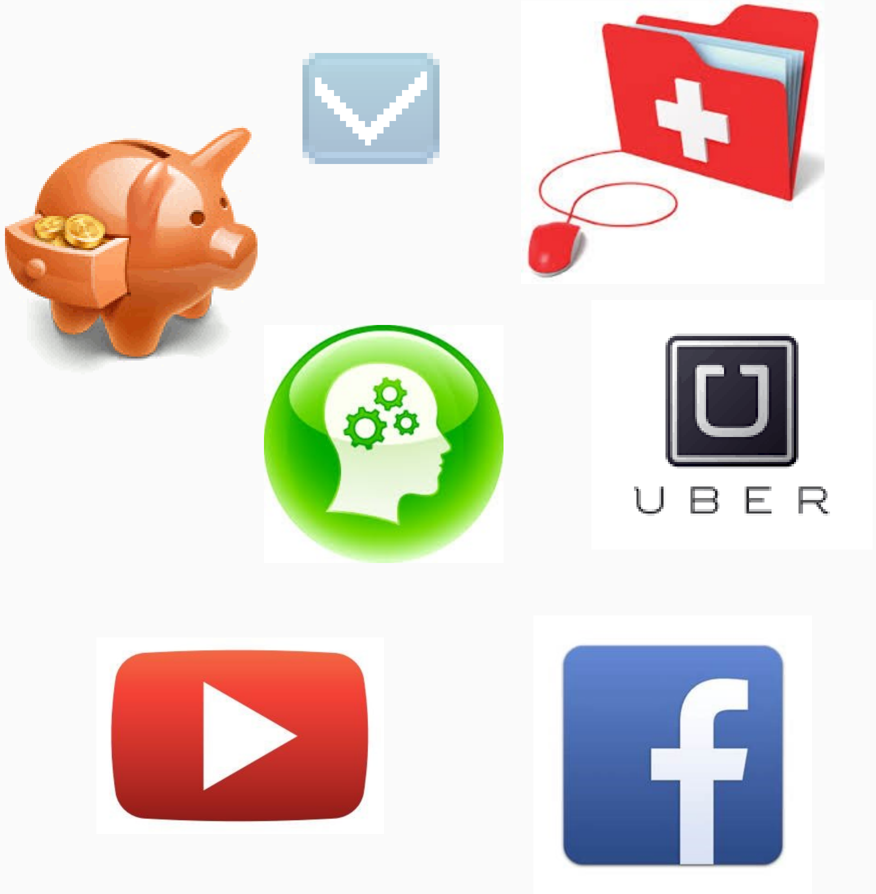
Disclaimer

Speaking in Personal Capacity

The Problem

We Keep Our Most Valuable Information Online

- Financial Information
- Communications
- Health Information
- Social Networks
- Intellectual Property
- Transportation
- Entertainment

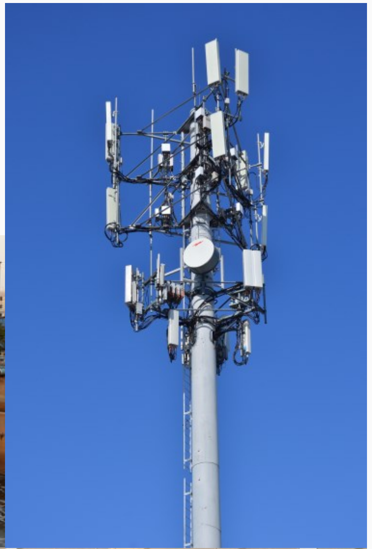


National Security Information is Likewise Readily Available in Digital Form

- Government Emails
- Government Networks
- Government "Soft Targets" (small agencies, municipalities)
- Defense Contractor Information
- Government Vendor Databases

Critical Infrastructure is Increasingly Networked

- Water
- Power/Energy
- Communications
- Emergency Services
- Healthcare
- Transportation



What were the core design concerns when we constructed the internet and the software that we use today?

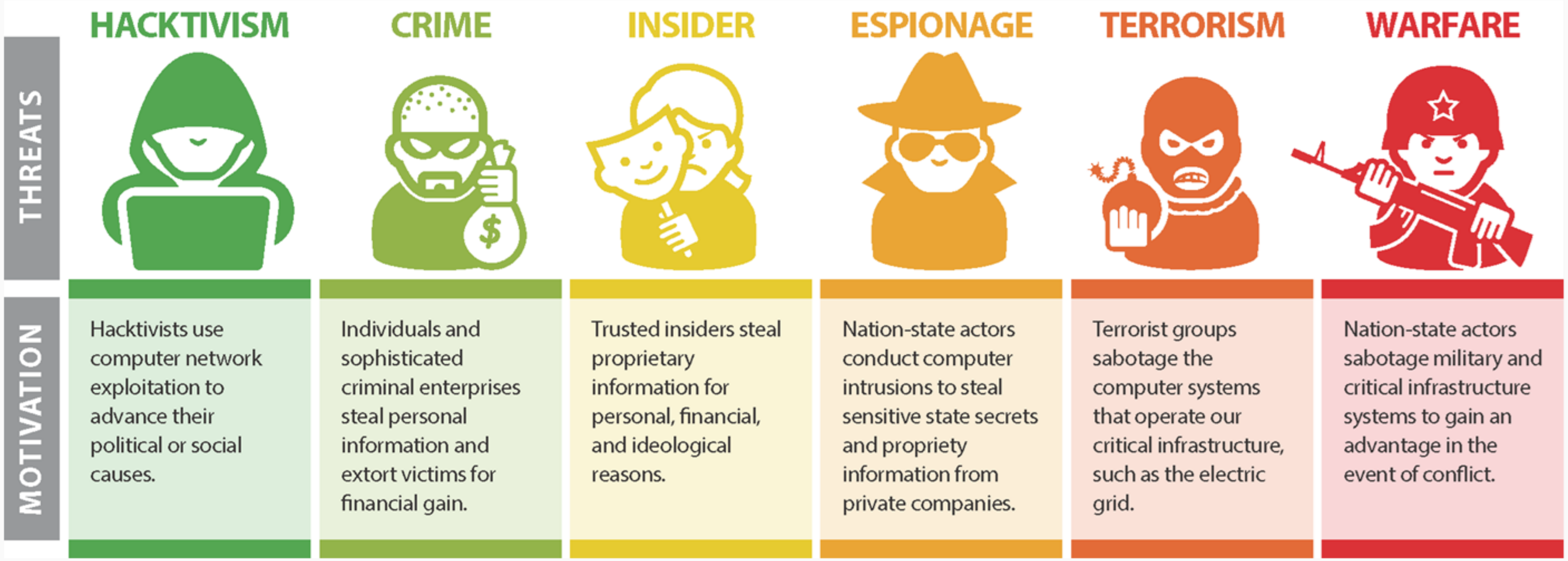
(1) *Functionality/Usability* (2) *Speed (time to market)* (3) *Cost*

Ferrari Chassis (~$3mil value)

Security, Resiliency, and Defensibility were an Afterthought

What have been the results?

Types of Hackers



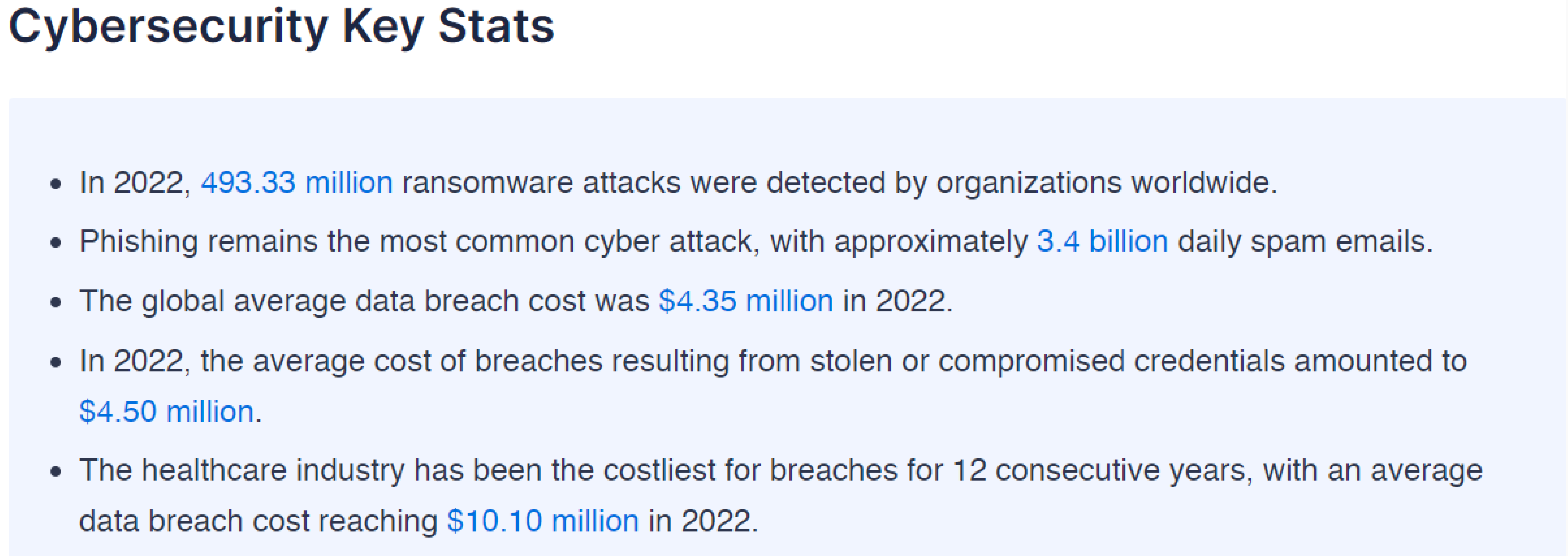
THREATS	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

Exclusive Title 18 Authority

Availability of Title 18 Authority

Title 50 Authority

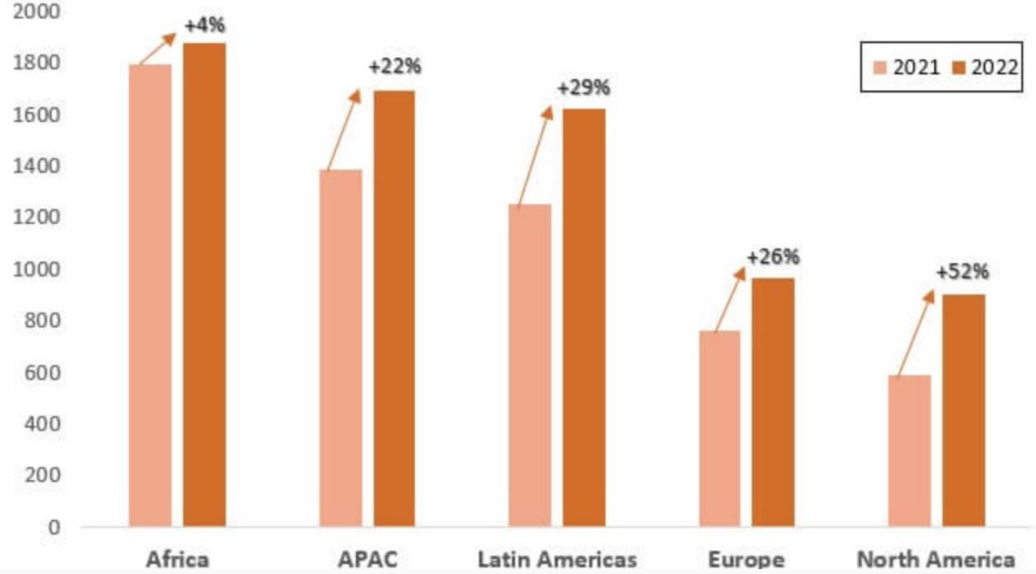
Title 10



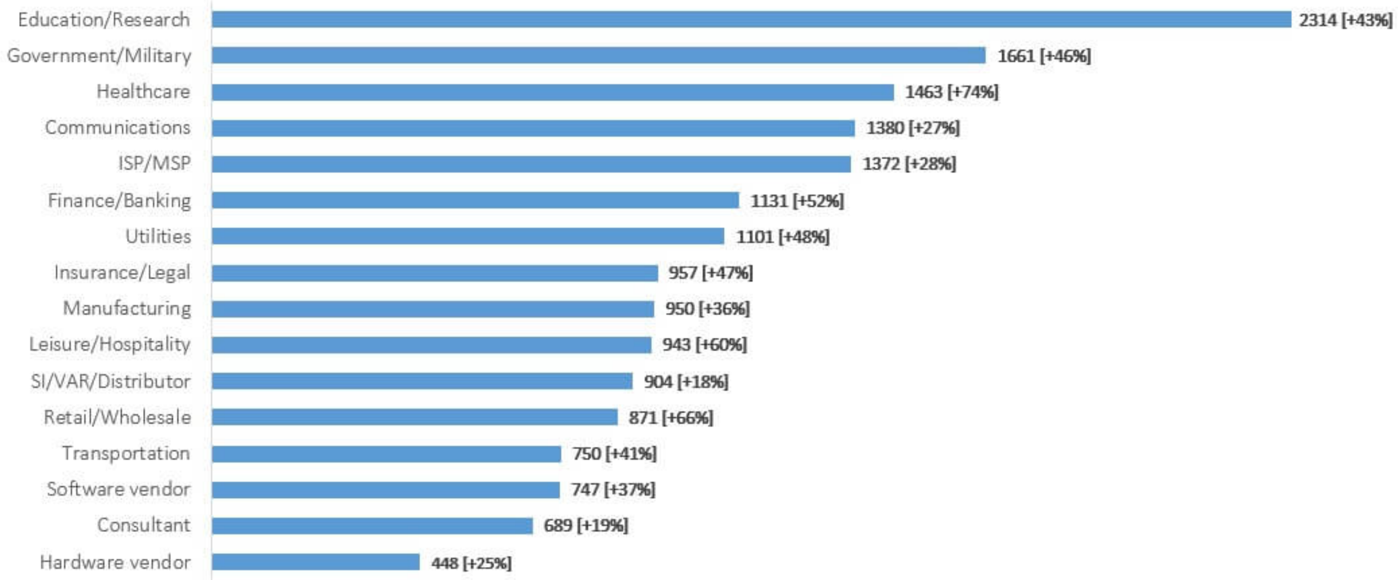
Cybersecurity Key Stats

- In 2022, 493.33 million ransomware attacks were detected by organizations worldwide.
- Phishing remains the most common cyber attack, with approximately 3.4 billion daily spam emails.
- The global average data breach cost was $4.35 million in 2022.
- In 2022, the average cost of breaches resulting from stolen or compromised credentials amounted to $4.50 million.
- The healthcare industry has been the costliest for breaches for 12 consecutive years, with an average data breach cost reaching $10.10 million in 2022.

Avg. Weekly Cyber Attacks per Organization by Region shows increase across all regions in 2022 compared to 2021



Avg. Weekly Cyber Attacks per Organinzation by Sector in 2022 showing all sectors suffer double-digit increase comapred to 2021



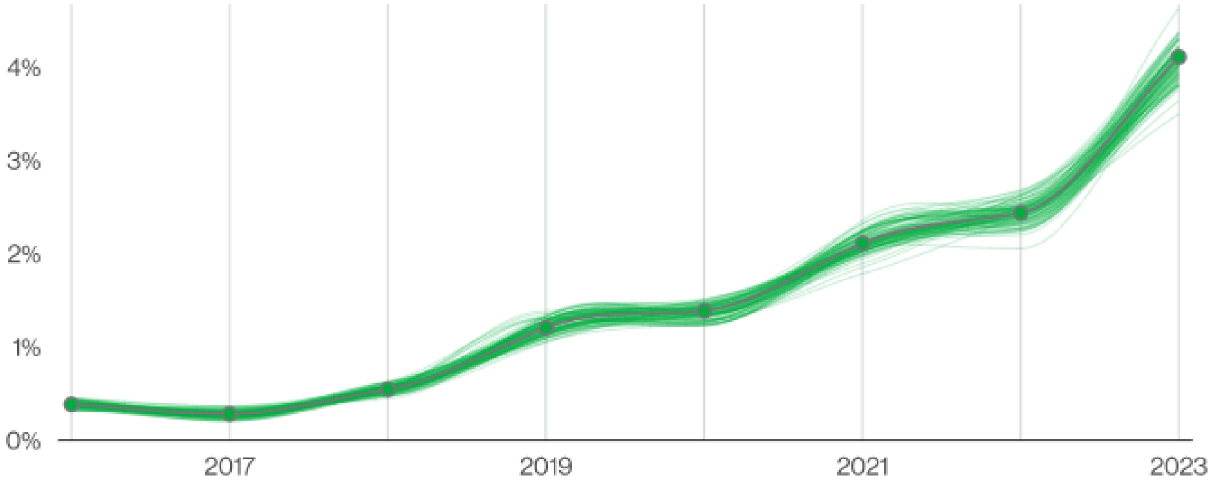


Figure 5. Pretexting incidents over time

Social Engineering attacks are often very effective and extremely lucrative for cybercriminals. Perhaps this is why Business Email Compromise (BEC) attacks (which are in essence pretexting attacks) have almost doubled across our entire incident dataset, as can be seen in Figure 5, and now represent more than 50% of incidents within the Social Engineering pattern.

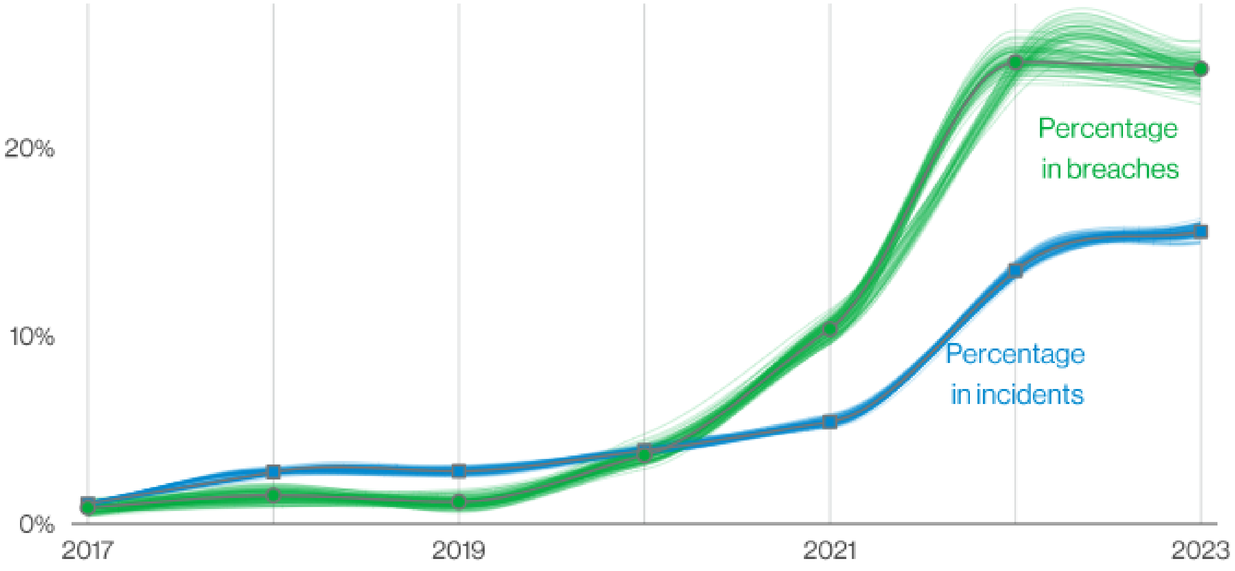
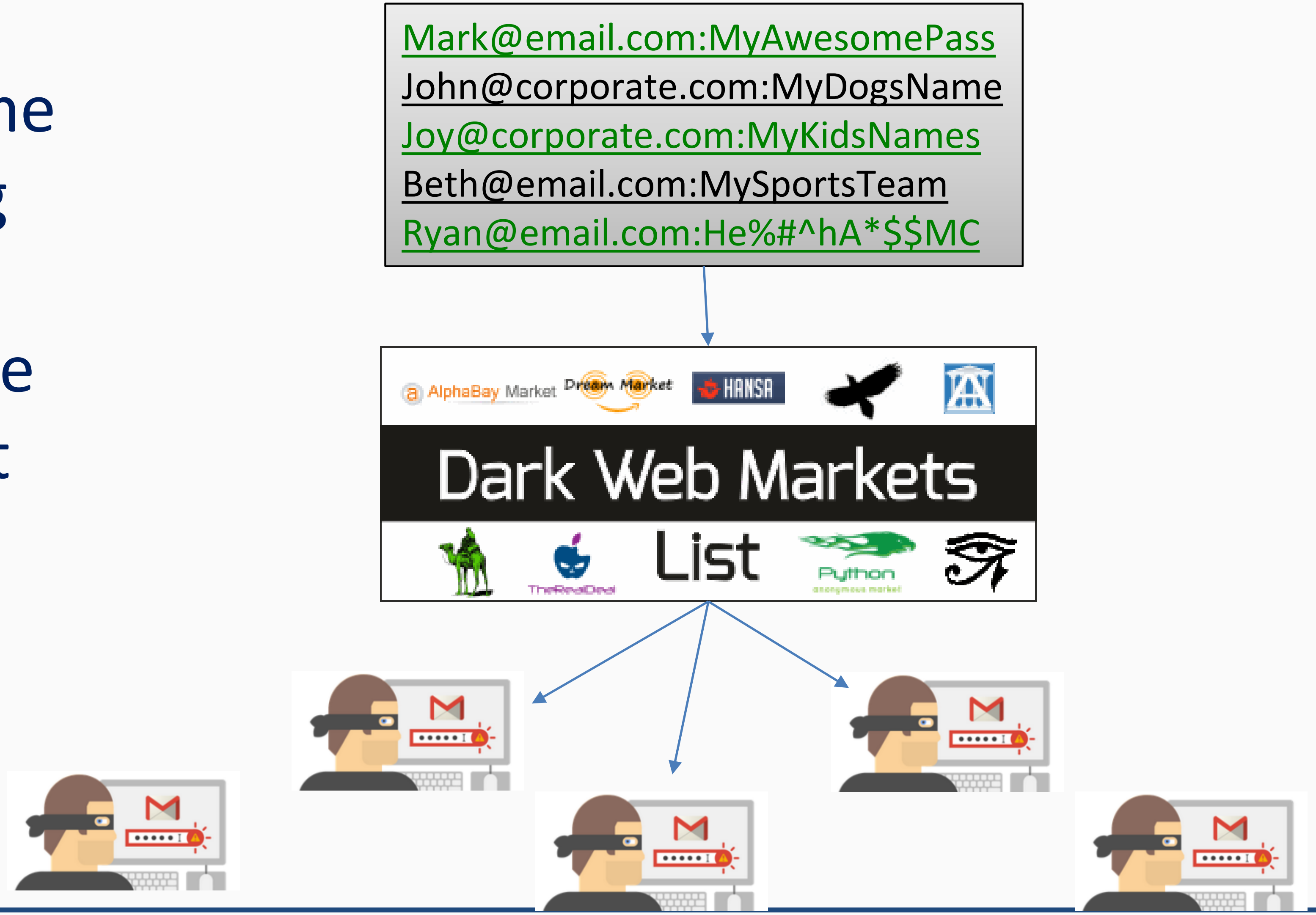


Figure 8. Ransomware action variety over time.

Ransomware continues its reign as one of the top Action types present in breaches, and while it did not actually grow, it did hold statistically steady at 24%. Ransomware is ubiquitous among organizations of all sizes and in all industries.

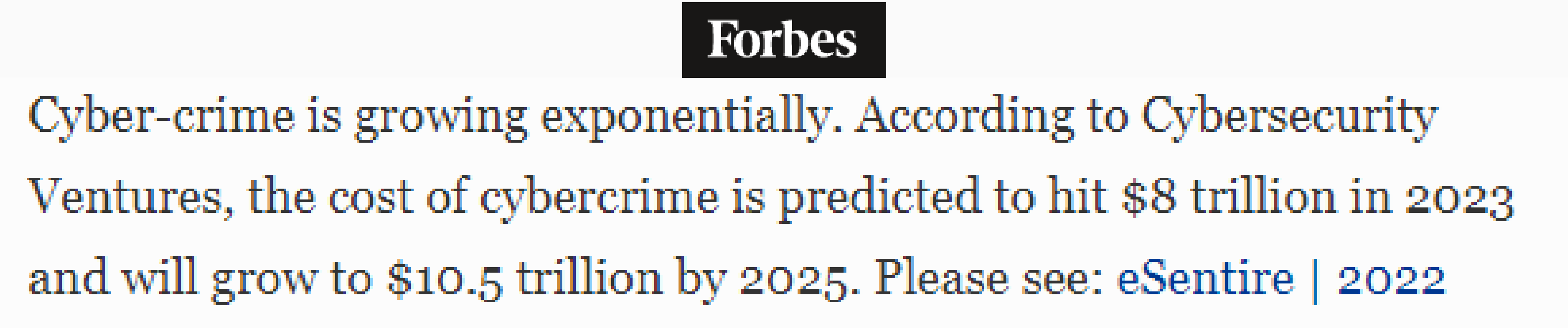
Cybercrime is Easy

- Most cybercrime tools (including user data) are readily available on the dark net



Mark@email.com:MyAwesomePass
John@corporate.com:MyDogsName
Joy@corporate.com:MyKidsNames
Beth@email.com:MySportsTeam
Ryan@email.com:He%#^hA*$$MC

Cost of Cybercrime

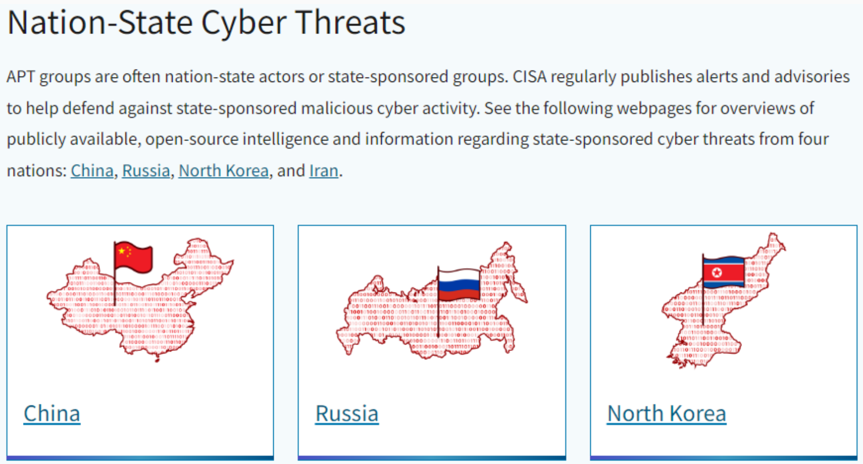


Forbes

Cyber-crime is growing exponentially. According to Cybersecurity Ventures, the cost of cybercrime is predicted to hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025. Please see: eSentire | 2022

- Global GDP in 2023 estimated to reach $112.6 trillion.
- Cybercrime costs about 7% of global GDP.
- By comparison, corruption costs ~5% of global GDP.

Nation State (APT) Cyberattacks



Nation-State Cyber Threats

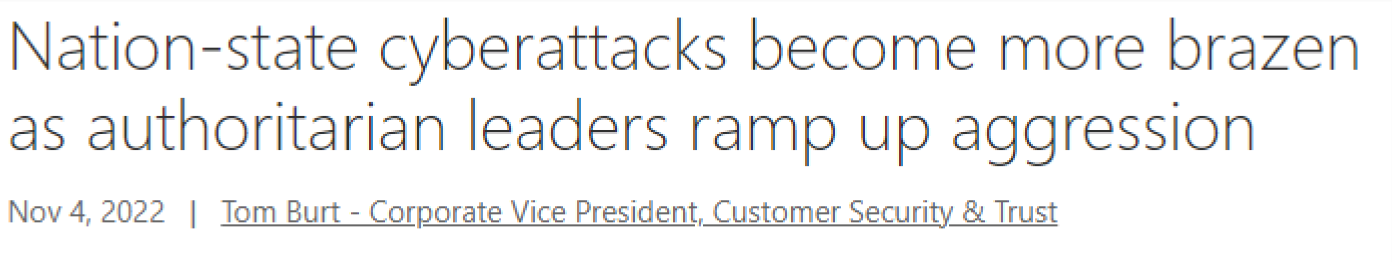
APT groups are often nation-state actors or state-sponsored groups. CISA regularly publishes alerts and advisories to help defend against state-sponsored malicious cyber activity. See the following webpages for overviews of publicly available, open-source intelligence and information regarding state-sponsored cyber threats from four nations: China, Russia, North Korea, and Iran.

China

Russia

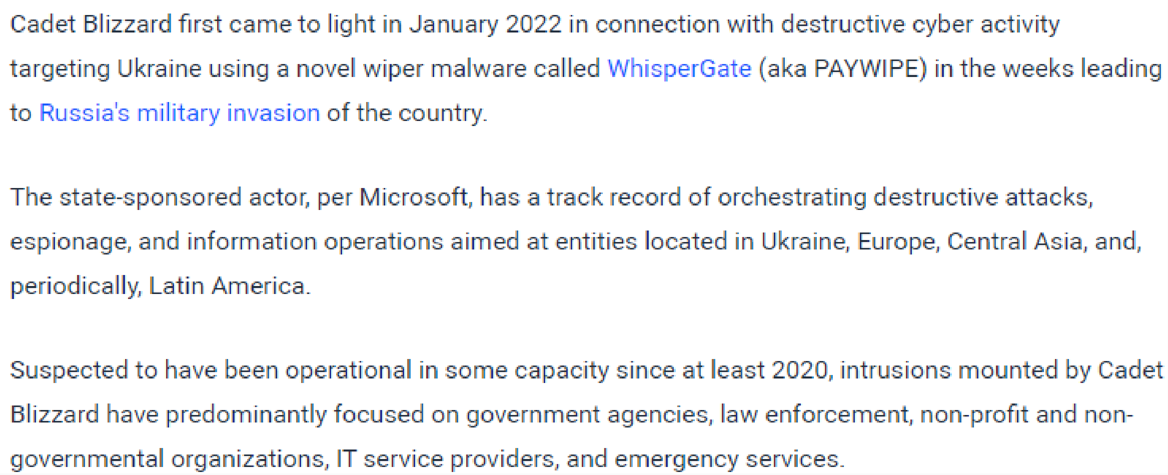
North Korea

Iran



Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression

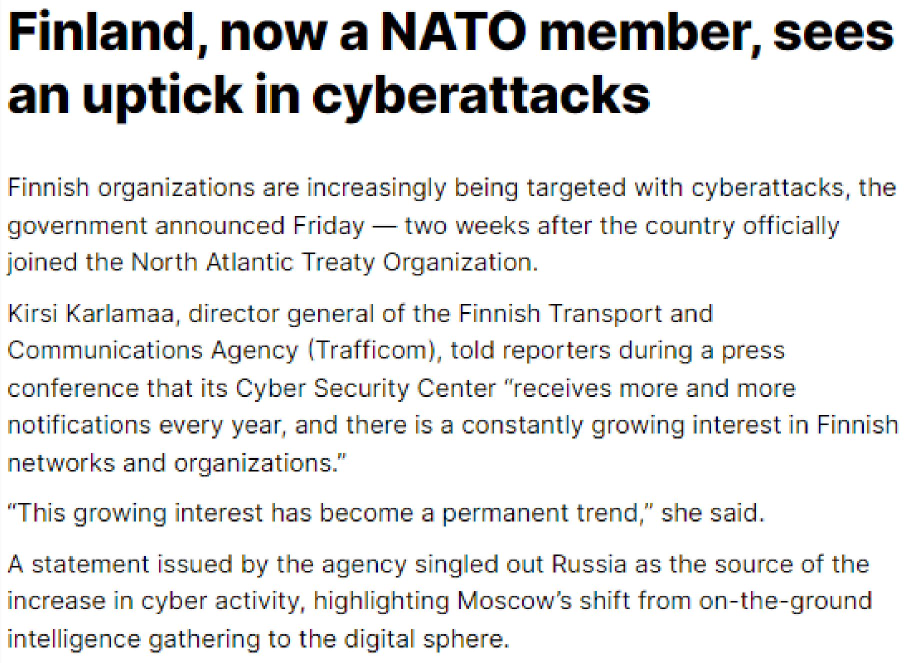
Nov 4, 2022 | Tom Burt - Corporate Vice President, Customer Security & Trust



Cadet Blizzard first came to light in January 2022 in connection with destructive cyber activity targeting Ukraine using a novel wiper malware called WhisperGate (aka PAYWIPE) in the weeks leading to Russia's military invasion of the country.

The state-sponsored actor, per Microsoft, has a track record of orchestrating destructive attacks, espionage, and information operations aimed at entities located in Ukraine, Europe, Central Asia, and, periodically, Latin America.

Suspected to have been operational in some capacity since at least 2020, intrusions mounted by Cadet Blizzard have predominantly focused on government agencies, law enforcement, non-profit and non-governmental organizations, IT service providers, and emergency services.



Finland, now a NATO member, sees an uptick in cyberattacks

Finnish organizations are increasingly being targeted with cyberattacks, the government announced Friday — two weeks after the country officially joined the North Atlantic Treaty Organization.

Kirsi Karlamaa, director general of the Finnish Transport and Communications Agency (Traficom), told reporters during a press conference that its Cyber Security Center "receives more and more notifications every year, and there is a constantly growing interest in Finnish networks and organizations."

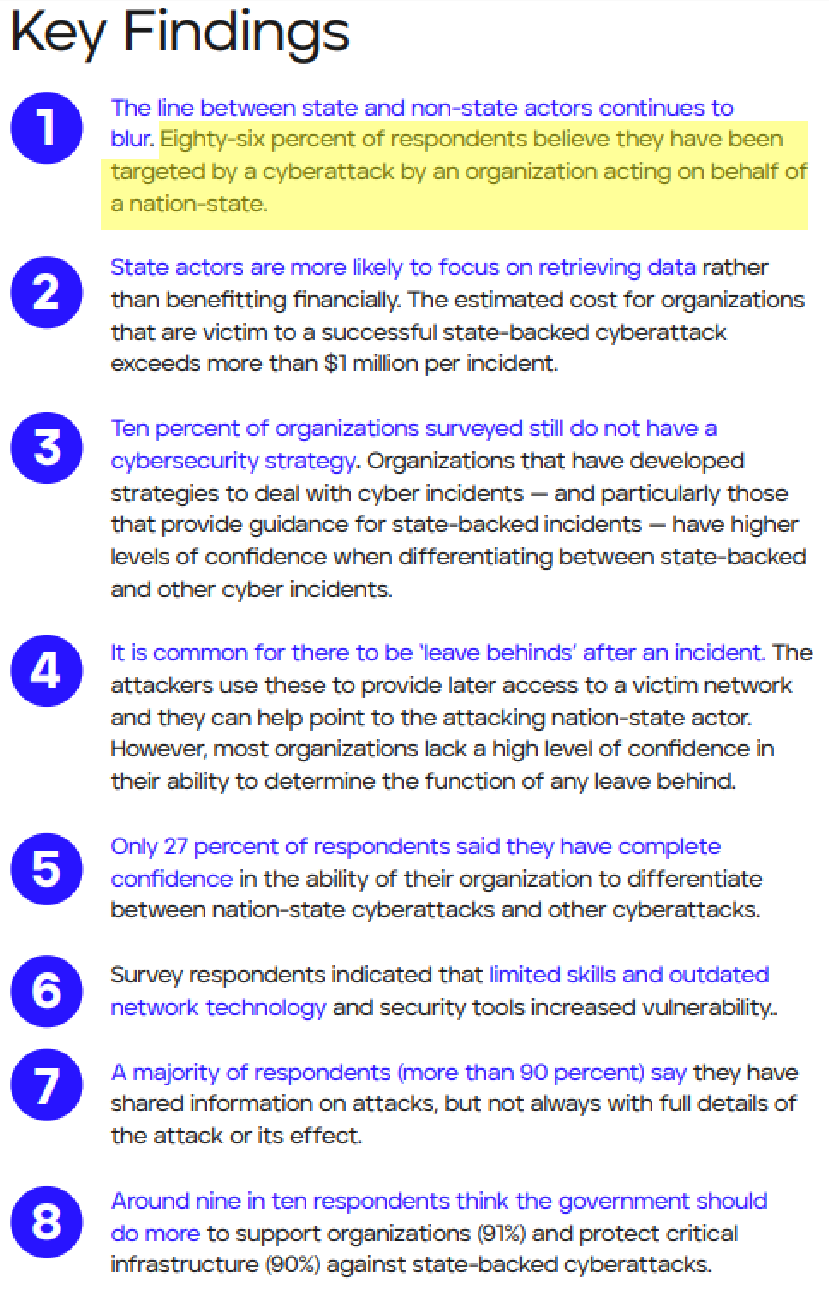
"This growing interest has become a permanent trend," she said.

A statement issued by the agency singled out Russia as the source of the increase in cyber activity, highlighting Moscow's shift from on-the-ground intelligence gathering to the digital sphere.

Trellix Global Threat Research

In the Crosshairs: Organizations and Nation-State Cyber Threats

Trellix



Key Findings

1. The line between state and non-state actors continues to blur. Eighty-six percent of respondents believe they have been targeted by a cyberattack by an organization acting on behalf of a nation-state.

2. State actors are more likely to focus on retrieving data rather than benefitting financially. The estimated cost for organizations that are victim to a successful state-backed cyberattack exceeds more than $1 million per incident.

3. Ten percent of organizations surveyed still do not have a cybersecurity strategy. Organizations that have developed strategies to deal with cyber incidents — and particularly those that provide guidance for state-backed incidents — have higher levels of confidence when differentiating between state-backed and other cyber incidents.

4. It is common for there to be 'leave behinds' after an incident. The attackers use these to provide later access to a victim network and they can help point to the attacking nation-state actor. However, most organizations lack a high level of confidence in their ability to determine the function of any leave behind.

5. Only 27 percent of respondents said they have complete confidence in the ability of their organization to differentiate between nation-state cyberattacks and other cyberattacks.

6. Survey respondents indicated that limited skills and outdated network technology and security tools increased vulnerability..

7. A majority of respondents (more than 90 percent) say they have shared information on attacks, but not always with full details of the attack or its effect.

8. Around nine in ten respondents think the government should do more to support organizations (91%) and protect critical infrastructure (90%) against state-backed cyberattacks.

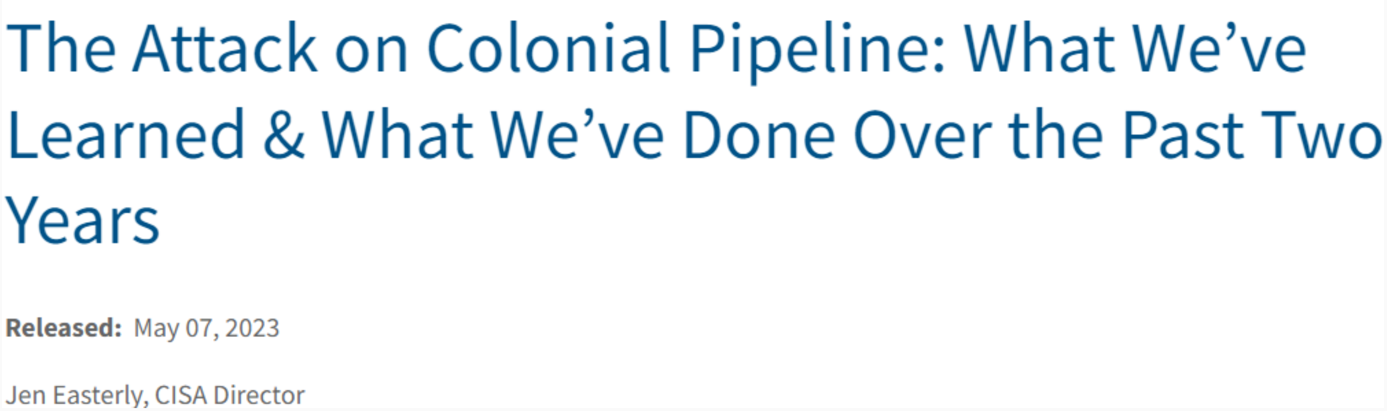
Nation State Cyberattacks can Spin Out of Control

- Security experts believe the attack originated from an update of a Ukrainian tax accounting package called MeDoc In a report published by Wired, a White House assessment pegged the total damages brought about by NotPetya to more than $10 billion.

- During the attack initiated on 27 June 2017, the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant went offline. Several Ukrainian ministries, banks and metro systems were also affected.

- Among those affected elsewhere included British advertising company WPP, Maersk Line, American pharmaceutical company Merck & Co. (internationally doing business as MSD), Russian oil company Rosneft (its oil production was unaffected), multinational law firm DLA Piper, French construction company Saint-Gobain and its retail and subsidiary outlets in Estonia, British consumer goods company Reckitt Benckiser, German personal care company Beiersdorf, German logistics company DHL, United States food company Mondelez International, American hospital operator Heritage Valley Health System, the Cadbury's Chocolate Factory in Hobart, Tasmania, JNPT, India's largest container port, and Princeton Community Hospital in rural West Virginia will scrap and replace its entire computer network on its path to recovery

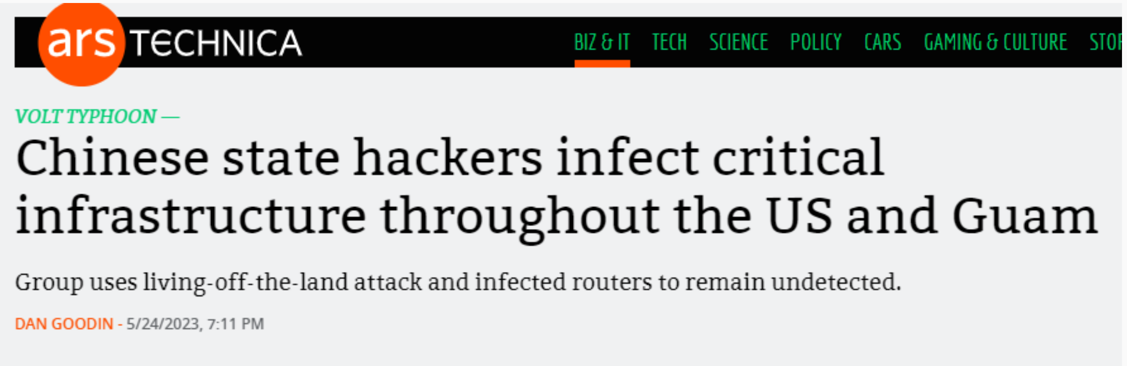
Cyberattacks on Critical Infrastructure



The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years

Released: May 07, 2023

Jen Easterly, CISA Director

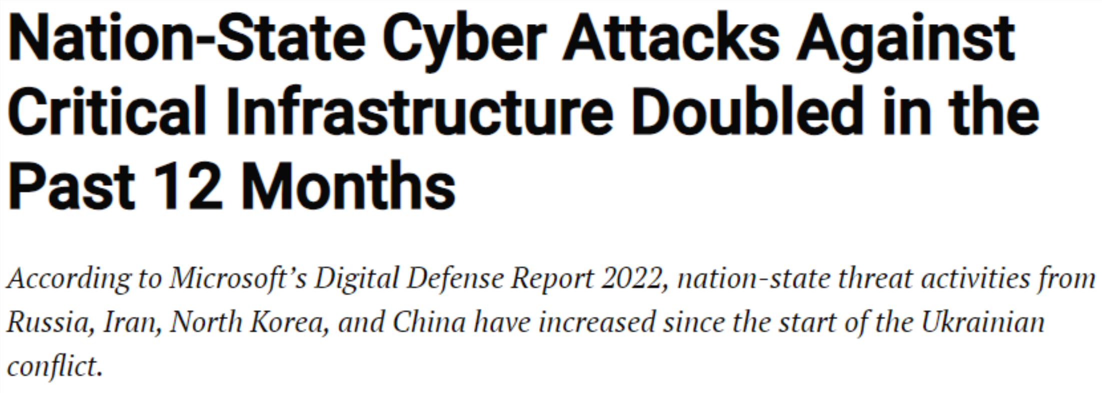


VOLT TYPHOON —

Chinese state hackers infect critical infrastructure throughout the US and Guam

Group uses living-off-the-land attack and infected routers to remain undetected.

DAN GOODIN - 5/24/2023, 7:11 PM



Nation-State Cyber Attacks Against Critical Infrastructure Doubled in the Past 12 Months

According to Microsoft's Digital Defense Report 2022, nation-state threat activities from Russia, Iran, North Korea, and China have increased since the start of the Ukrainian conflict.

The Proposed Solution

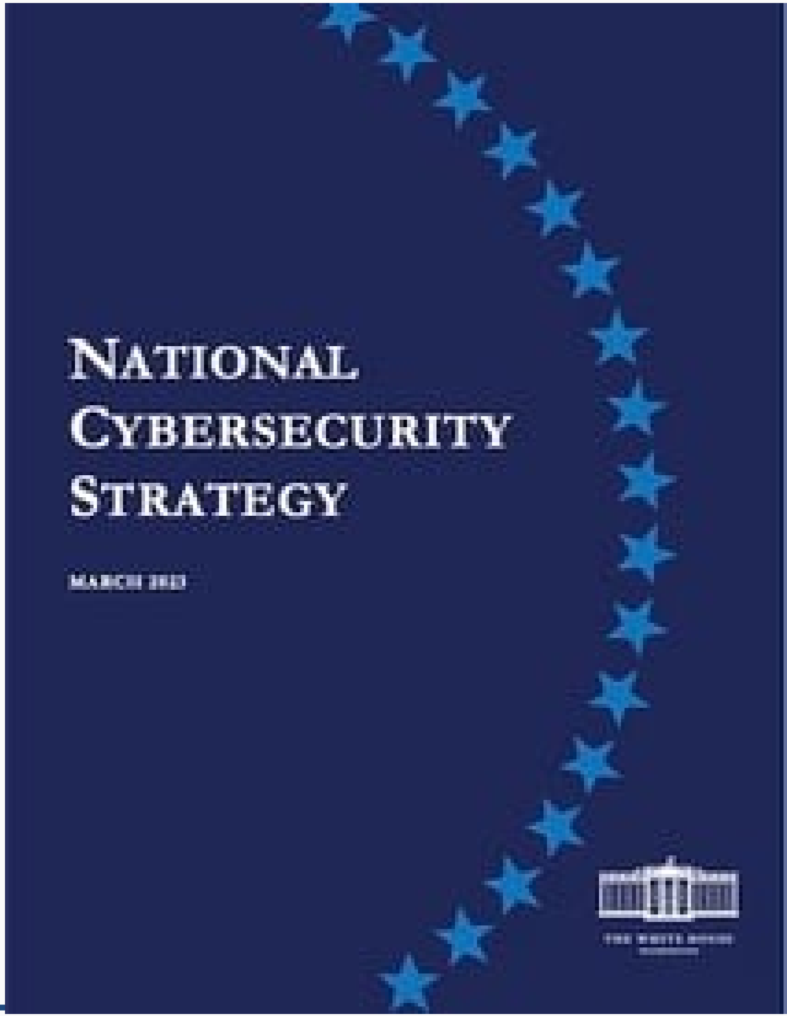
National Cybersecurity Strategy

NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

What is the National Cybersecurity Strategy?

- Presidentially-approved foundational policy.
- “United States will reimagine cyberspace as a tool to achieve our goals in a way that reflects our values: economic security and prosperity; respect for human rights and fundamental freedoms; trust in our democracy and democratic institutions; and an equitable and diverse society. To realize this vision, we must make fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace.”



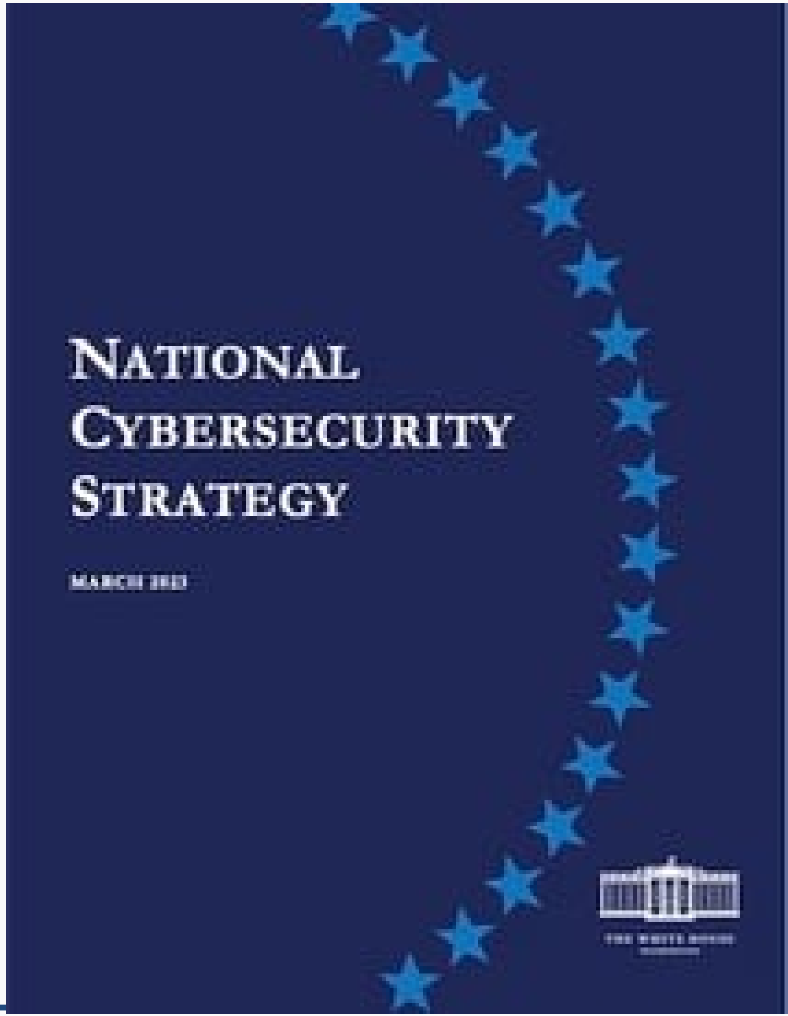
NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

THE WHITE HOUSE

Strategy Development Process

- Internal ONCD Process
- Interagency Process
- Public Sector Input
- Partner Input

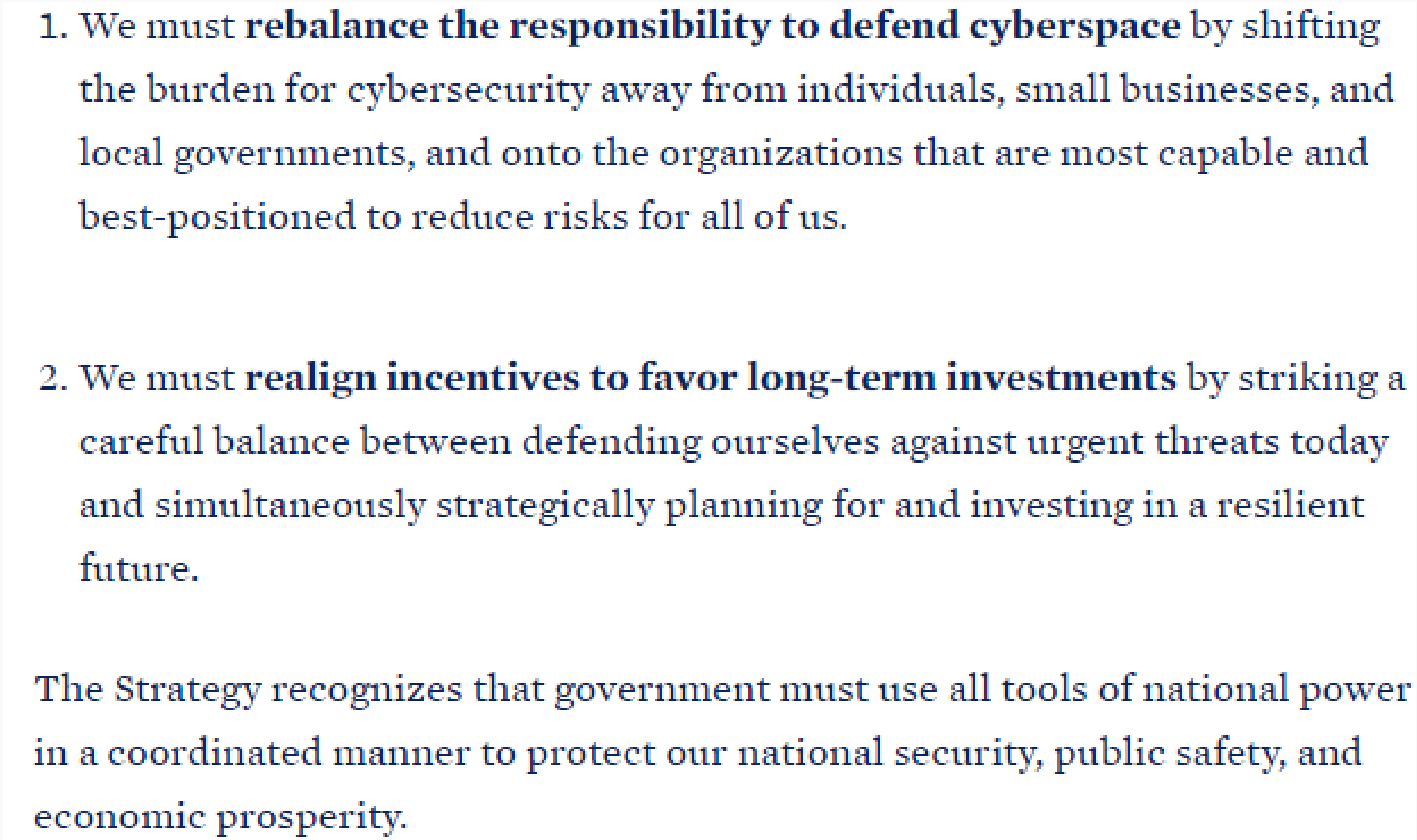


NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

THE WHITE HOUSE

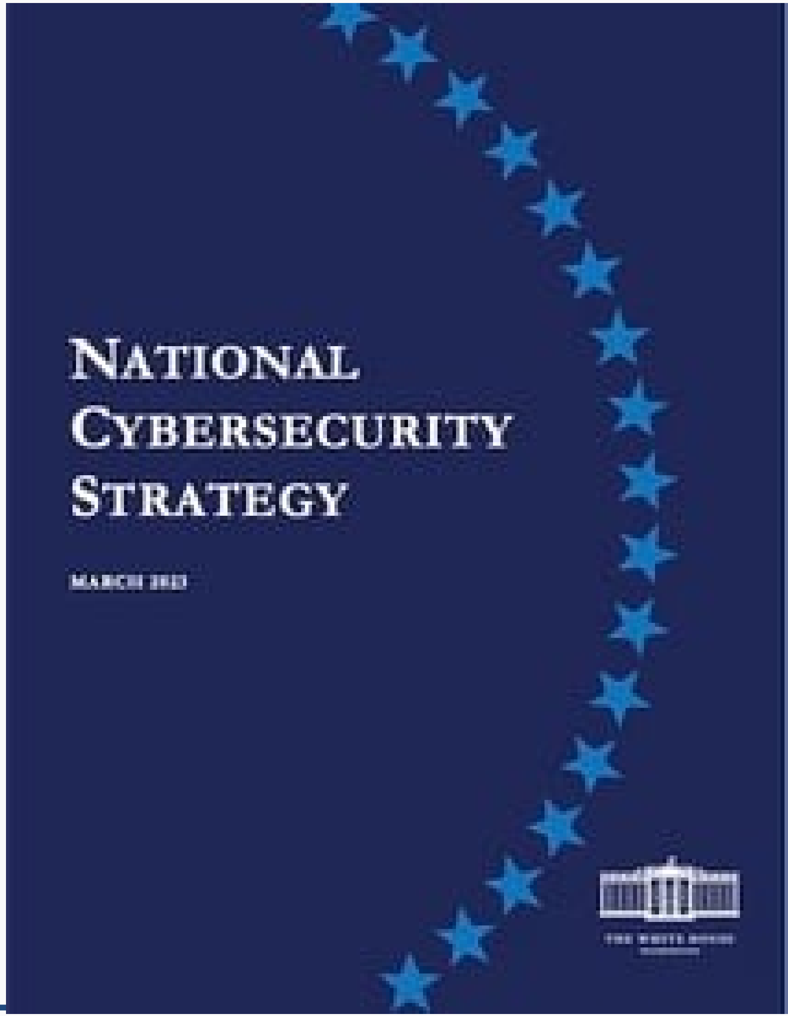
Summary - Two Fundamental Pivots



1. We must **rebalance the responsibility to defend cyberspace** by shifting the burden for cybersecurity away from individuals, small businesses, and local governments, and onto the organizations that are most capable and best-positioned to reduce risks for all of us.

2. We must **realign incentives to favor long-term investments** by striking a careful balance between defending ourselves against urgent threats today and simultaneously strategically planning for and investing in a resilient future.

The Strategy recognizes that government must use all tools of national power in a coordinated manner to protect our national security, public safety, and economic prosperity.



NATIONAL CYBERSECURITY STRATEGY

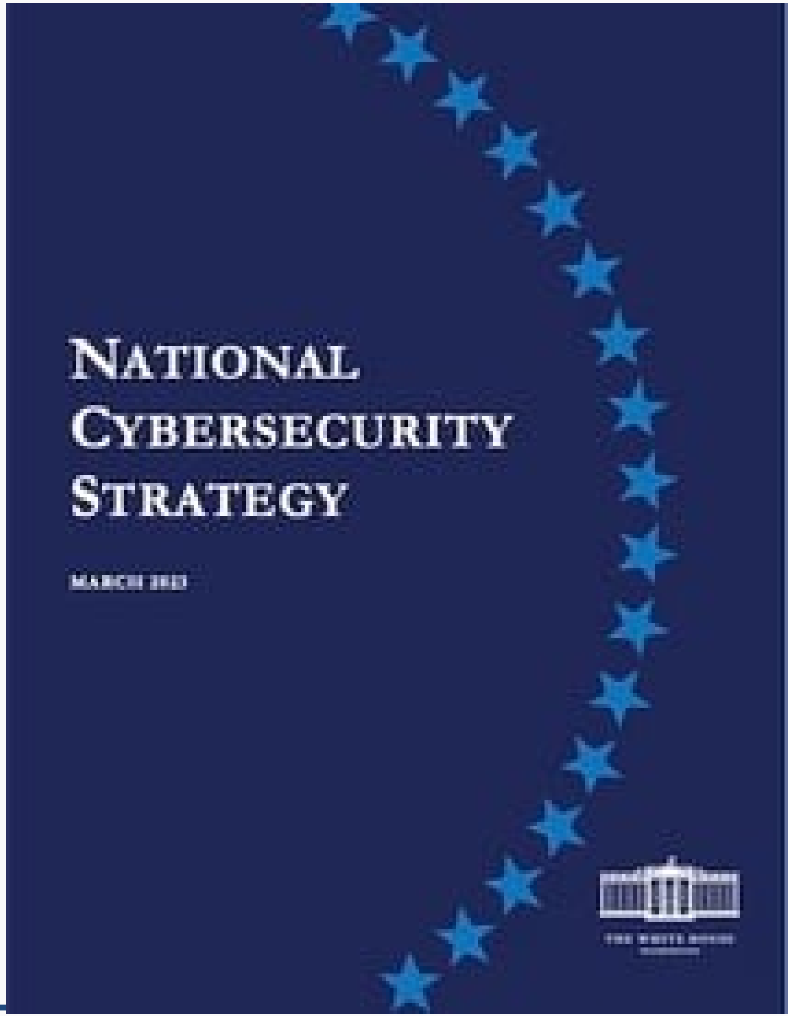
MARCH 2023

THE WHITE HOUSE

Fundamental Pivot #1

(1) Shift responsibility and burden of cybersecurity to those best able to bear it.

- “A single person’s momentary lapse in judgment, use of an outdated password, or errant click on a suspicious link should not have national security consequences”
- “protecting data and ensuring reliability of critical systems must be the responsibility of the owners and operators of the systems that hold our data and make our society function, as well as of the technology providers that build and service these systems.”



NATIONAL CYBERSECURITY STRATEGY

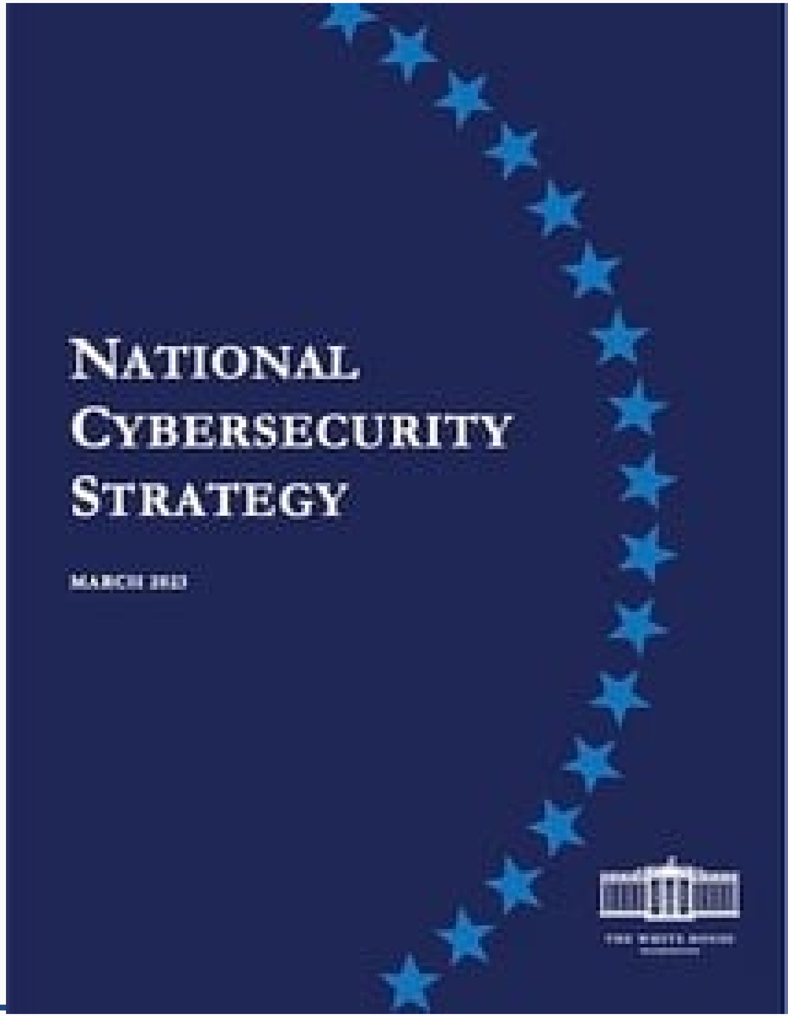
MARCH 2023

THE WHITE HOUSE

Fundamental Pivot #2

(2) Realign incentives to favor long-term resiliency while still defending system we have at present.

- “We must ensure that market forces and public programs alike reward security and resilience, build a robust and diverse cyber workforce, embrace security and resilience by design, strategically coordinate research and development investments in cybersecurity, and promote the collaborative stewardship of our digital ecosystem”
- Streamlining regulations



NATIONAL CYBERSECURITY STRATEGY

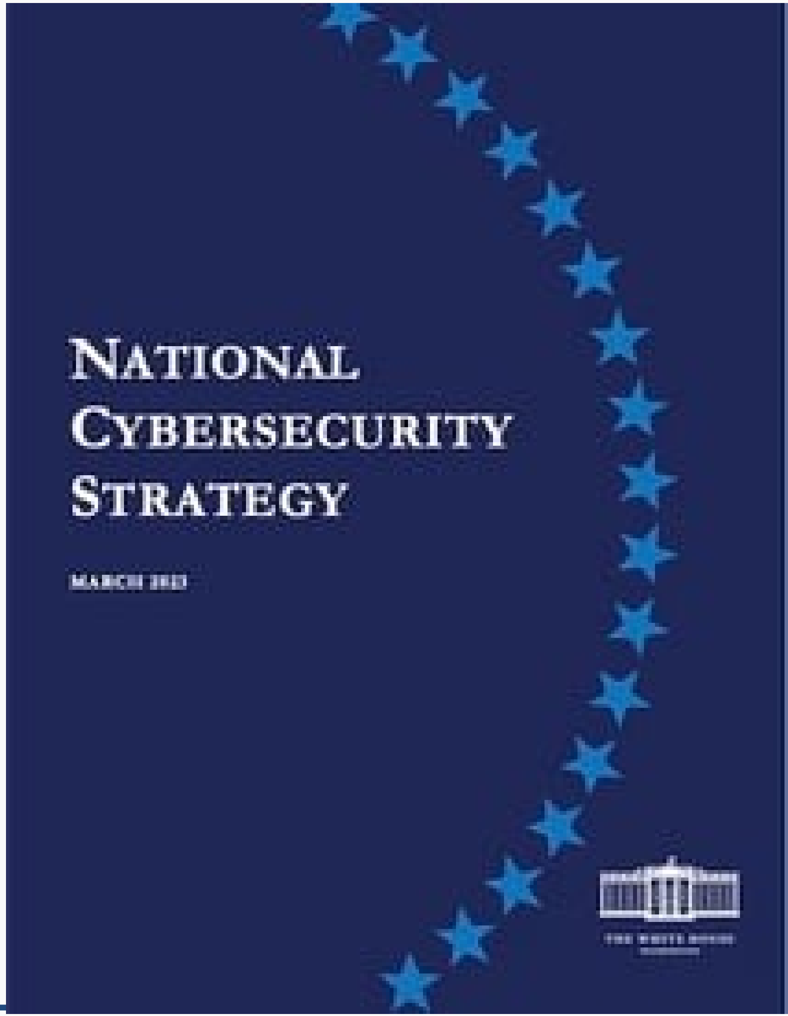
MARCH 2023

THE WHITE HOUSE

Summary - Foundational Goals

Digital ecosystem that is:

- *Defensible*, where cyber defense is overwhelmingly easier, cheaper, and more effective;
- *Resilient*, where cyber incidents and errors have little widespread or lasting impact; and,
- *Values-aligned*, where our most cherished values shape—and are in turn reinforced by—our digital world.



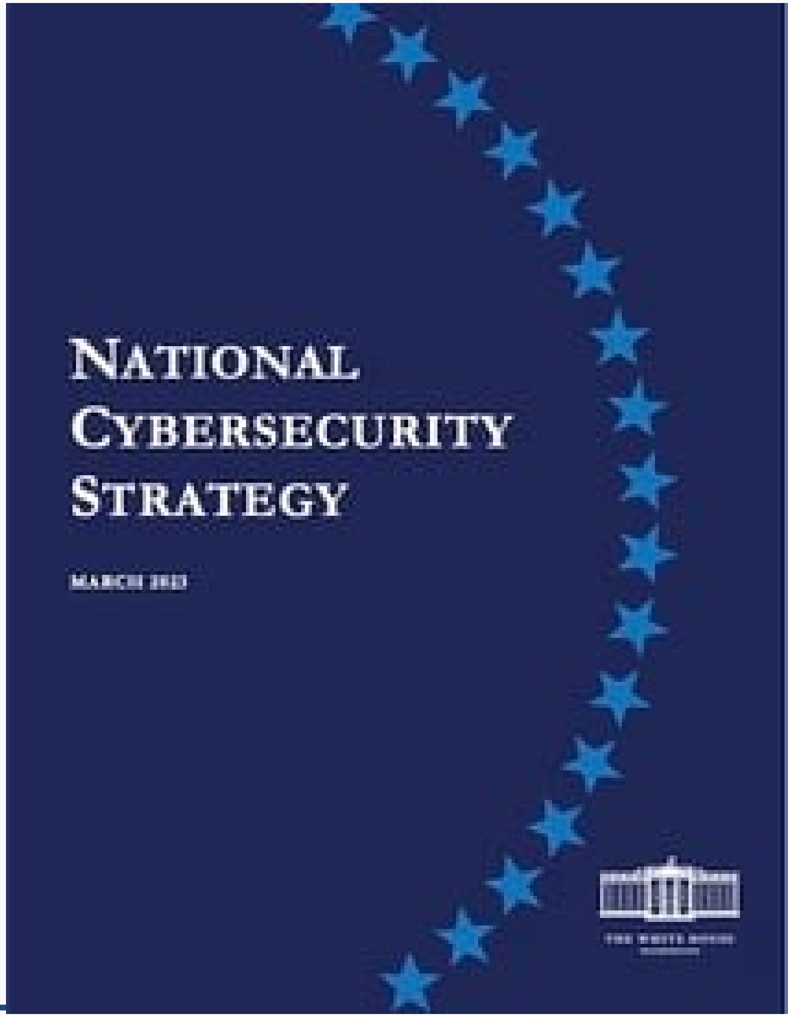
NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

THE WHITE HOUSE

Shift in Thinking: Public-Private Collaboration

- Shift in thinking: we are all in this together
- Specific examples: JCDC, NSA Cybersecurity Collaboration Center
- White House: Space Forum, Electric Vehicle Forum, Health Forum



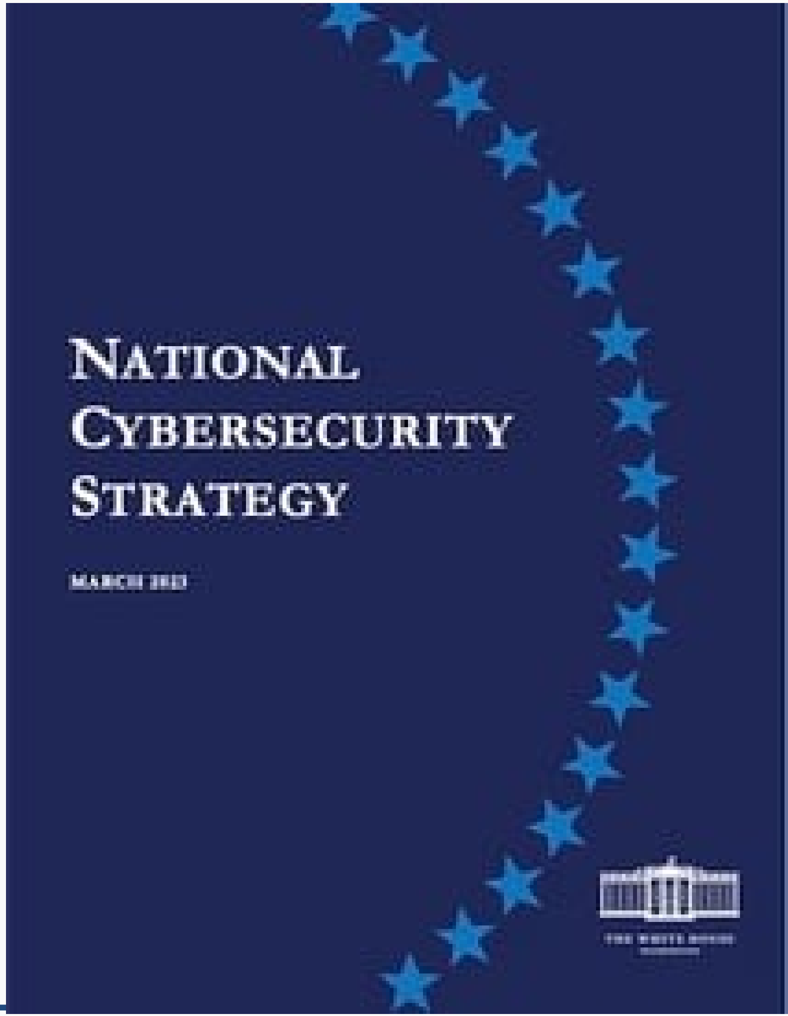
NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

THE WHITE HOUSE

Summary - Five Pillars

1. Defend Critical Infrastructure
2. Disrupt and Dismantle Threat Actors
3. Shape Market Forces to Drive Security and Resilience
4. Invest in a Resilient Future
5. Forge International Partnerships to Pursue Shared Goals



NATIONAL CYBERSECURITY STRATEGY

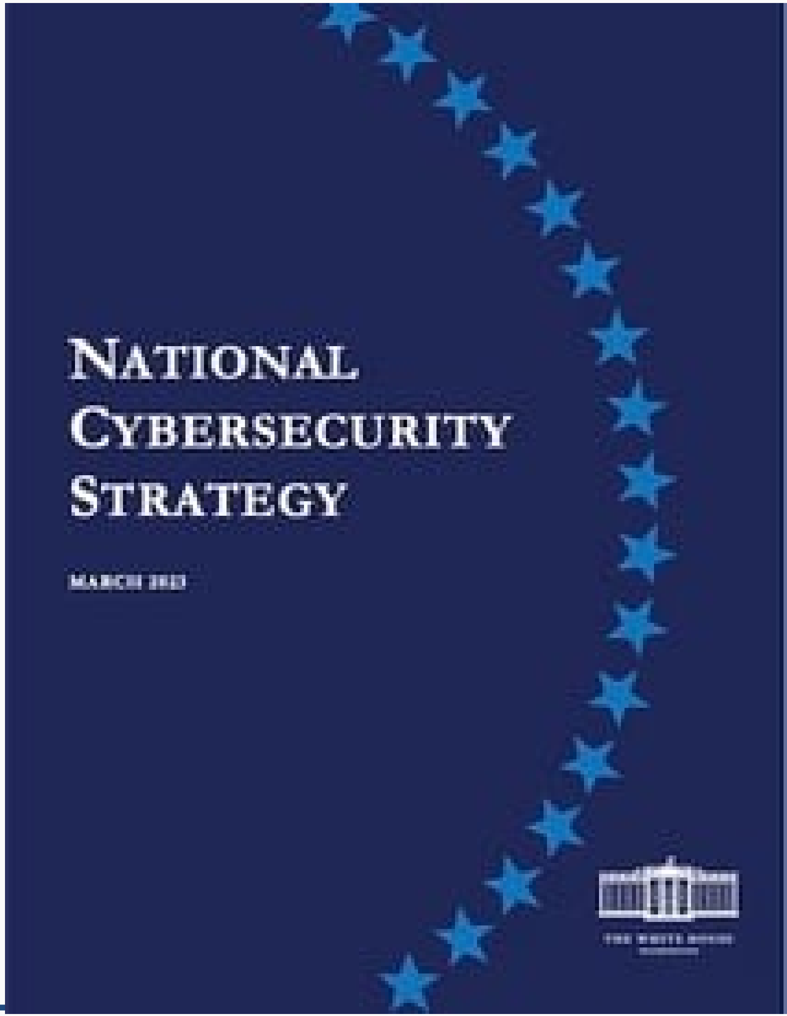
MARCH 2023

THE WHITE HOUSE

Pillar 1

Defend Critical Infrastructure – We will give the American people confidence in the availability and resilience of our critical infrastructure and the essential services it provides, including by:

- Expanding the use of minimum cybersecurity requirements in critical sectors to ensure national security and public safety and harmonizing regulations to reduce the burden of compliance;
- Enabling public-private collaboration at the speed and scale necessary to defend critical infrastructure and essential services; and,
- Defending and modernizing Federal networks and updating Federal incident response policy.



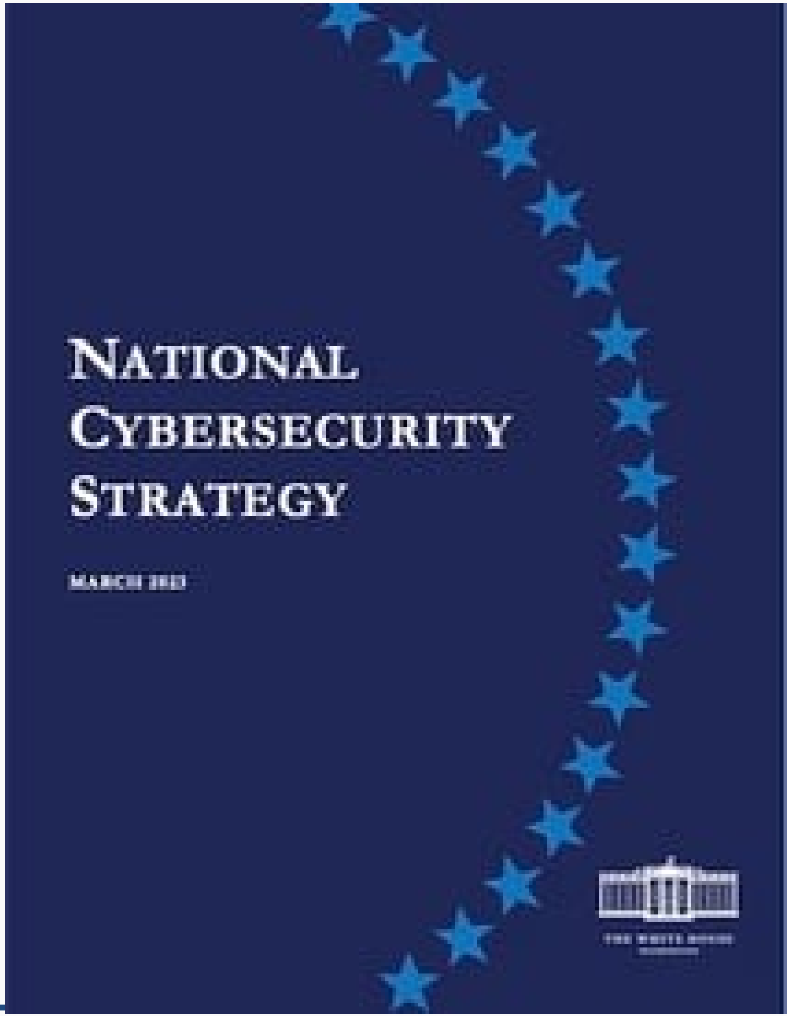
NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

Pillar 2

Disrupt and Dismantle Threat Actors – Using all instruments of national power, we will make malicious cyber actors incapable of threatening the national security or public safety of the United States, including by:

- Strategically employing all tools of national power to disrupt adversaries;
- Engaging the private sector in disruption activities through scalable mechanisms; and,
- Addressing the ransomware threat through a comprehensive Federal approach and in lockstep with our international partners.



NATIONAL CYBERSECURITY STRATEGY

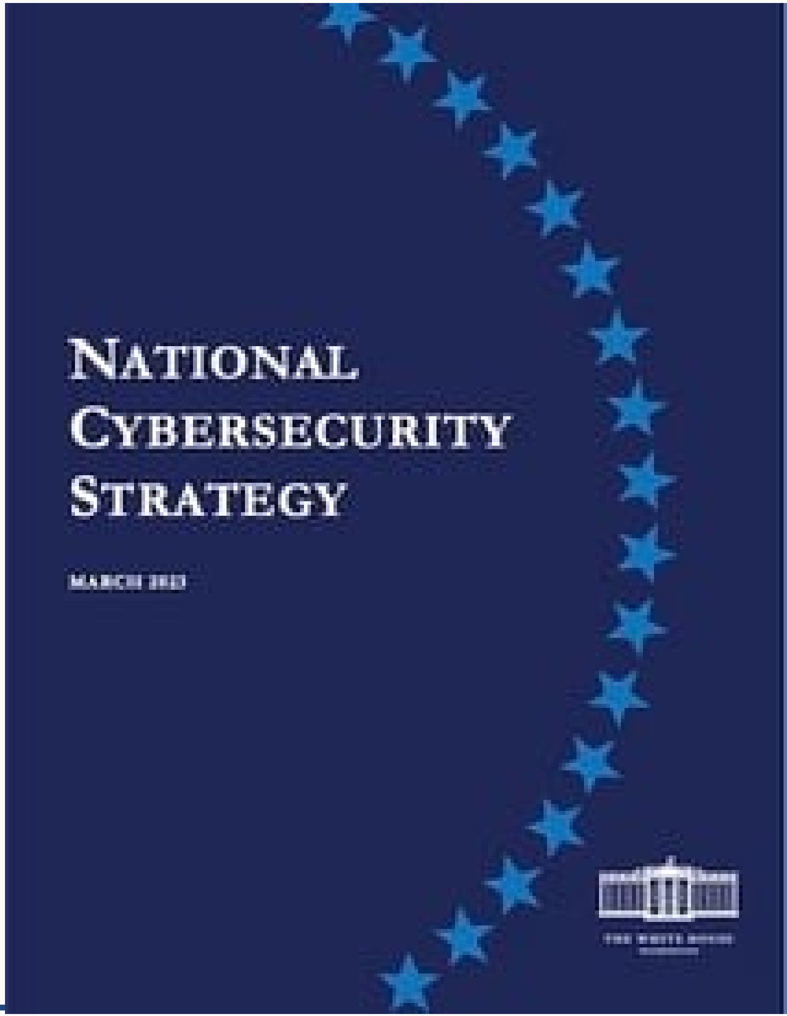
MARCH 2023

THE WHITE HOUSE

Pillar 3

Shape Market Forces to Drive Security and Resilience – We will place responsibility on those within our digital ecosystem that are best positioned to reduce risk and shift the consequences of poor cybersecurity away from the most vulnerable in order to make our digital ecosystem more trustworthy, including by:

- Promoting privacy and the security of personal data;
- Shifting liability for software products and services to promote secure development practices; and,
- Ensuring that Federal grant programs promote investments in new infrastructure that are secure and resilient.



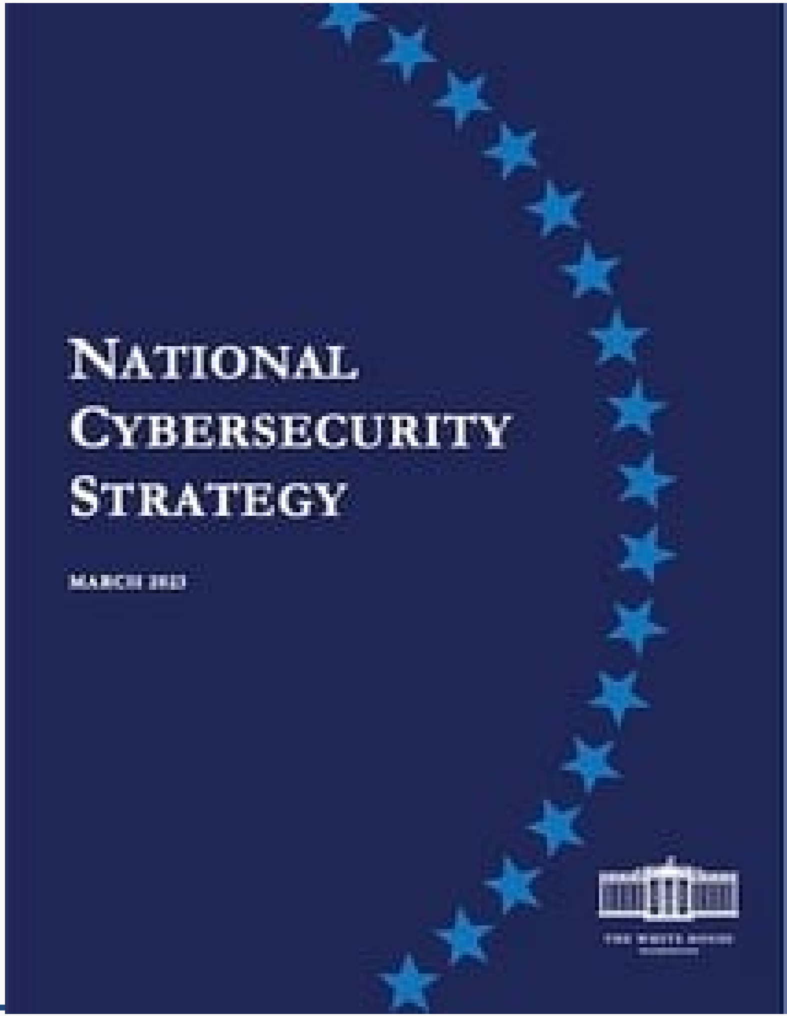
NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

Pillar 4

Invest in a Resilient Future – Through strategic investments and coordinated, collaborative action, the United States will continue to lead the world in the innovation of secure and resilient next-generation technologies and infrastructure, including by:

- Reducing systemic technical vulnerabilities in the foundation of the Internet and across the digital ecosystem while making it more resilient against transnational digital repression;
- Prioritizing cybersecurity R&D for next-generation technologies such as postquantum encryption, digital identity solutions, and clean energy infrastructure; and,
- Developing a diverse and robust national cyber workforce.



NATIONAL CYBERSECURITY STRATEGY

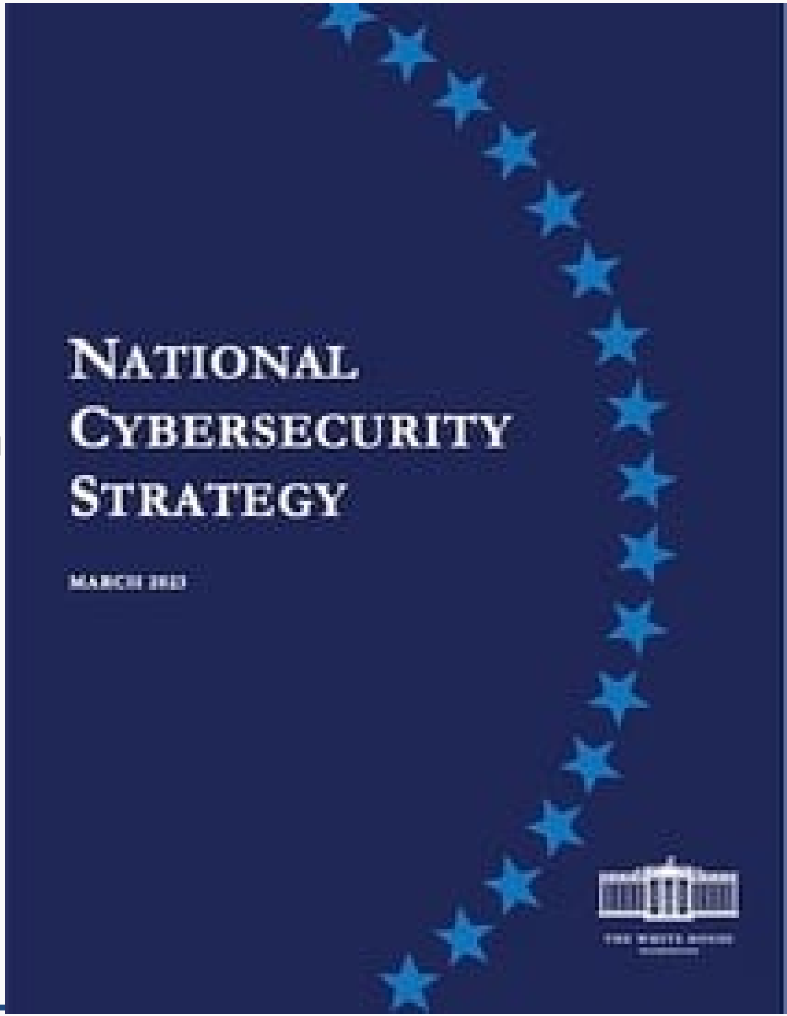
MARCH 2023

THE WHITE HOUSE

Pillar 5

Forge International Partnerships to Pursue Shared Goals – The United States seeks a world where responsible state behavior in cyberspace is expected and reinforced and where irresponsible behavior is isolating and costly, including by:

- Leveraging international coalitions and partnerships among like-minded nations to counter threats to our digital ecosystem through joint preparedness, response, and cost imposition;
- Increasing the capacity of our partners to defend themselves against cyber threats, both in peacetime and in crisis; and,
- Working with our allies and partners to make secure, reliable, and trustworthy global supply chains for information and communications technology and operational technology products and services.



NATIONAL CYBERSECURITY STRATEGY

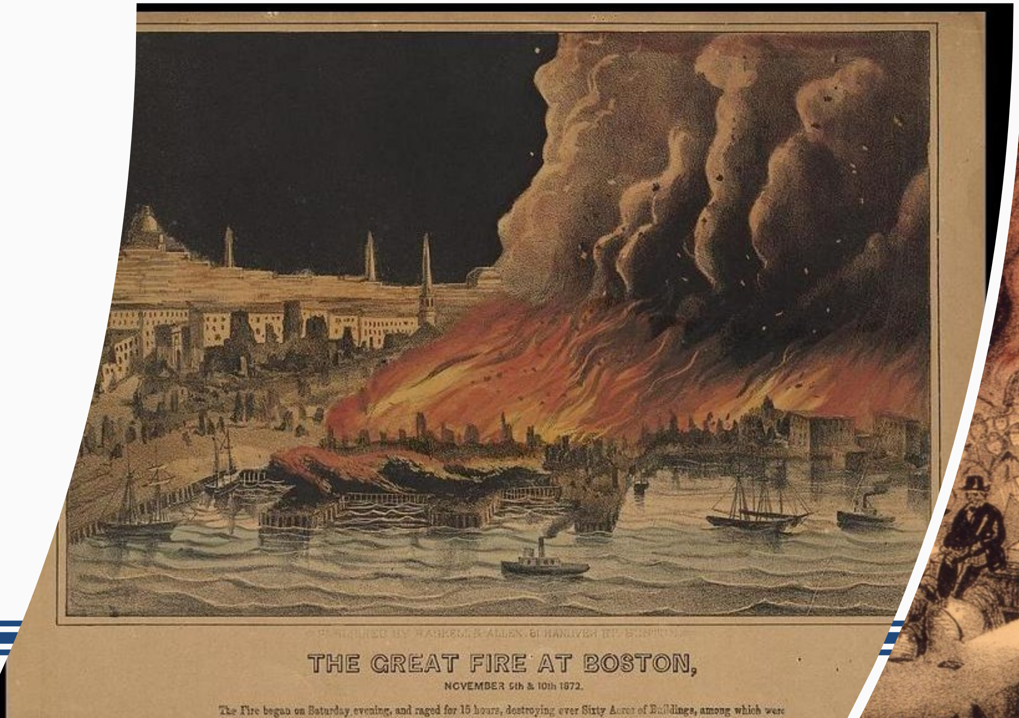
MARCH 2023

THE WHITE HOUSE

A Final Example

What do Urban Fires ("conflagrations") in the 1800s have to do with Cybersecurity?

- Massive, deadly fires were increasingly common in cities throughout 1800s.
- Why did it happen?
- How did open societies stop it when private property and individual action were the root causes?


PUBLISHED BY HASKELL & ALLEN, 61 HANOVER ST. BOSTON.
THE GREAT FIRE AT BOSTON,
NOVEMBER 9th & 10th 1872.
The Fire began on Saturday evening, and raged for 15 hours, destroying over Sixty Acres of Buildings, among which were

Conflagrations

- Boston suffered conflagrations in 1653, 1679, 1711, 1760, 1824, 1825, 1835, and 1872. The 1872 fire destroyed 776 buildings, with losses of ~$1.832 billion in 2023 dollars.
- The Great Chicago Fire resulted in 2,100 acres and 17,000 buildings burned to ash, with over $200 million (~$7.64 billion in 2023 dollars) in property and over 300 lives lost.
- Five conflagrations destroyed a major part of a large metropolis: New York in 1835, Chicago in 1871, Boston in 1872, Baltimore in 1904, and San Francisco in 1906.
- Building Designs in the 1800s were focused on speed and cost, rather than safety.
- City design was focused on ease of access, rather than security/safety.

How did Liberal Democracies Stop the Great Fires?

- A: A transformation in responsibility and accountability across society

1. Building Fire Codes (robust safety by design)
2. Building Material Fire Safety Regulations (supply chain)
3. Urban Planning Presuming Fires will Occur (architectural and city planning)
4. Lawsuits Available to Sue Manufacturers and Owners who Fail to Comply with Safety Rules (holding responsible parties accountable)
5. Insurance Companies Mandating Security Standards (revising standards)
6. Training on Fire Safety at Work and Schools (everyone trained on minimum necessary safety)
7. Firefighting Specialists Trained and Retained (experts who address acute risks)
8. Firefighters Receive Quality Equipment (funding our defenders)
9. Technological Progress (incentivizing tech that prevented fire)

Liberal Democracies Overcome Challenges by Harnessing the Power of Citizens and the Market through Incentives while Retaining Core Rights

How can Liberal Democracies Stop Cyberattacks?

- A: A transformation in responsibility and accountability across society

1. Robust Security by Design (memory safe languages)
2. Minimum Hardware/Software Safety Standards (supply chain/ SBOM)
3. Resilient Network Architecture (zero trust network defense)
4. Lawsuits Available to Sue Manufacturers and Owners who Fail to Comply with Safety Rules (holding responsible parties accountable)
5. Insurance Companies Mandating Security Standards (revising standards)
6. Training on Cyber Safety at Work and Schools (baseline for the many)
7. Network Security Specialists Trained and Retained (quality network defenders as core to an organization as firefighters are to a city)
8. Network Defenders Receive Quality Equipment (funding our defenders)
9. Technological Progress (incentivizing products that enhance cybersecurity)
10. Robust Cooperation Mechanisms for Asset and Threat Response Agencies

Questions