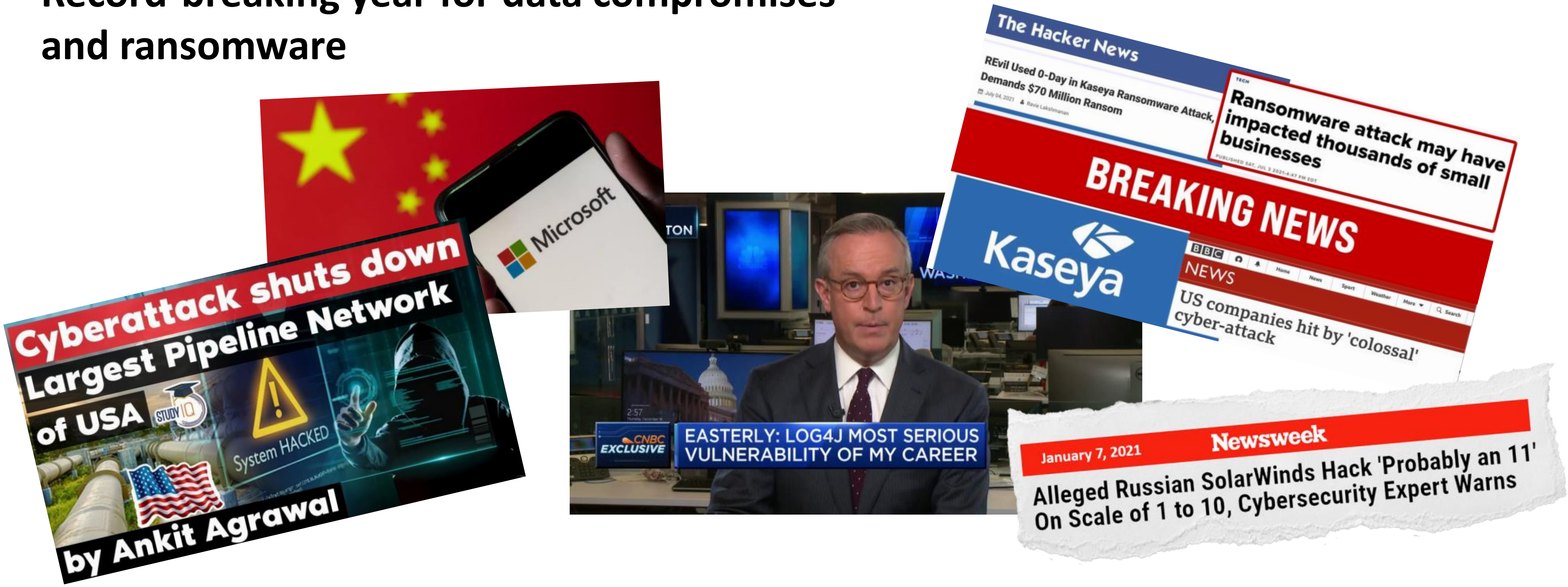
NATIONAL ASSOCIATION OF
WHOLESALER-DISTRIBUTORS

Cybersecurity: Protecting Your Future

Chris Feeney – President, BITS

Bank Policy Institute

Record-breaking year for data compromises and ransomware



Cyberattack shuts down Largest Pipeline Network of USA by Ankit Agrawal

EASTERLY: LOG4J MOST SERIOUS VULNERABILITY OF MY CAREER

The Hacker News

REvil Used 0-Day in Kaseya Ransomware Attack, Demands $70 Million Ransom

Ransomware attack may have impacted thousands of small businesses

BREAKING NEWS

US companies hit by 'colossal' cyber-attack

Newsweek

January 7, 2021

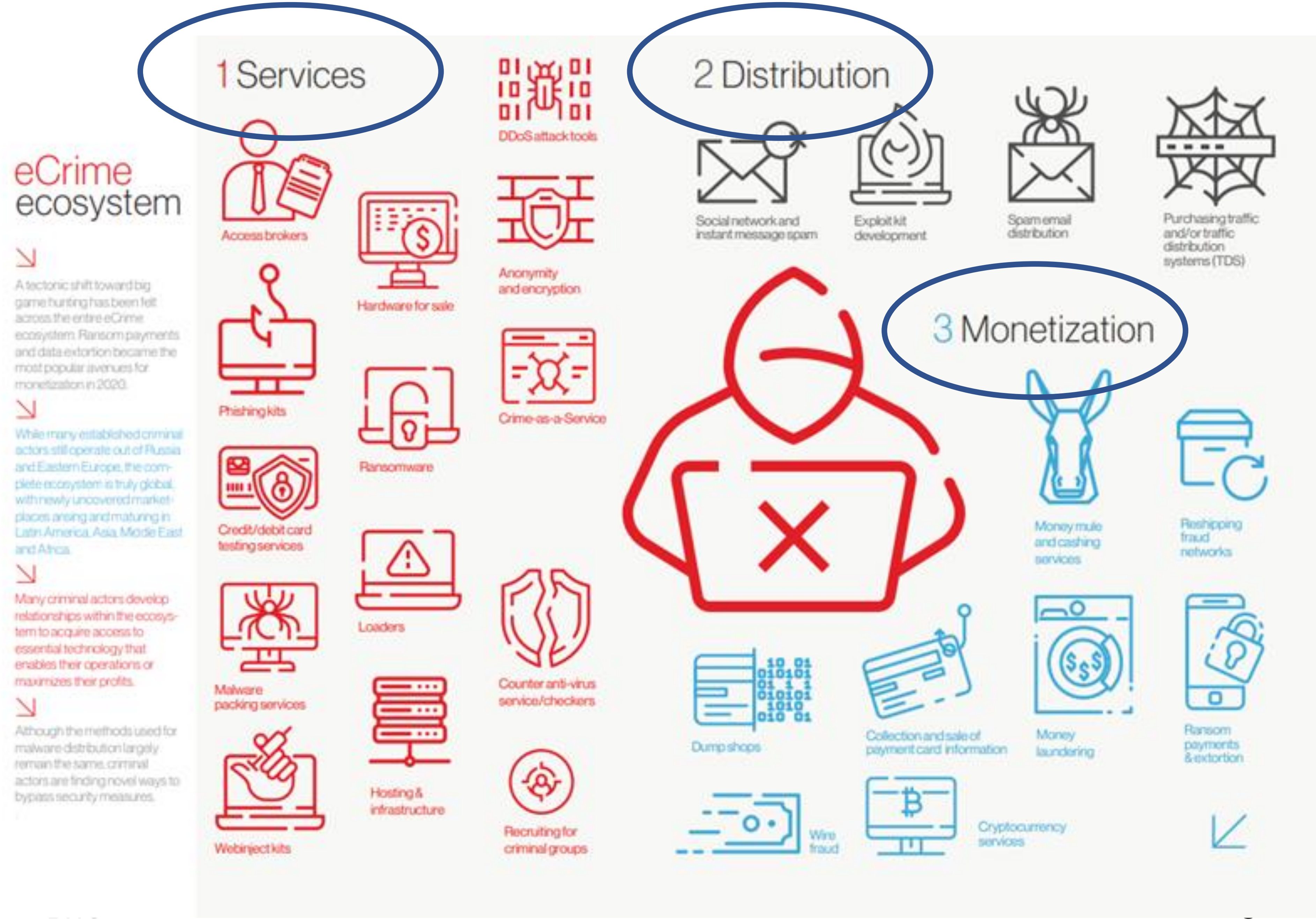
Alleged Russian SolarWinds Hack 'Probably an 11' On Scale of 1 to 10, Cybersecurity Expert Warns

What we see in the news is just the tip of the iceberg…

The first half of 2021 saw a **102% increase in ransomware attacks** compared to the beginning of 2020. (Check Point, 2021)

50% of organizations encountered **ransomware-related activity** (Cisco, 2021)

bpi
BITS



eCrime ecosystem

A tectonic shift toward big game hunting has been felt across the entire eCrime ecosystem. Ransom payments and data extortion became the most popular avenues for monetization in 2020.

While many established criminal actors still operate out of Russia and Eastern Europe, the complete ecosystem is truly global, with newly uncovered marketplaces arising and maturing in Latin America, Asia, Middle East and Africa.

Many criminal actors develop relationships within the ecosystem to acquire access to essential technology that enables their operations or maximizes their profits.

Although the methods used for malware distribution largely remain the same, criminal actors are finding novel ways to bypass security measures.

1 Services
Access brokers
Phishing kits
Credit/debit card testing services
Malware packing services
Webinject kits
Hardware for sale
Ransomware
Loaders
Hosting & infrastructure
DDoS attack tools
Anonymity and encryption
Crime-as-a-Service
Counter anti-virus service/checkers
Recruiting for criminal groups
2 Distribution
Social network and instant message spam
Exploit kit development
Spam email distribution
Purchasing traffic and/or traffic distribution systems (TDS)
3 Monetization
Money mule and cashing services
Reshipping fraud networks
Dump shops
Collection and sale of payment card information
Money laundering
Ransom payments & extortion
Wire fraud
Cryptocurrency services

Source: CrowdStrike's 2021 Global Threat Report

Ransomware – High Impact & Growing

Ransomware is a financially motivated extortion attack that encrypts data to effectively shut down access to systems by legitimate users until (presumably) a ransom is paid. In recent months, ransomware attacks on critical infrastructures have emphasized the potentially significant business impact and resulting need to protect against these threats.

What's different?

Shift to Ransomware-as-a-Service

Ransomware attacks have shifted from simple malware affecting a single system to targeted operations run as a "service" by cybercriminals or a gang of active attackers who attempt to infiltrate and exploit the entire enterprise. These attacks can navigate complex networks and mask their behavior, continuing to threaten business operations long after the initial encounter.

Increased Sophistication of Attacks

Attackers are using more sophisticated business models that include both advanced technological techniques (i.e., zero-day technical exploits) to gain enterprise control, deny access to, and exfiltrate data and an evaluation of the targeted business in order to set ransom prices based on the company's financial documentation, cyber-insurance coverage levels, and/or regulatory compliance fines.

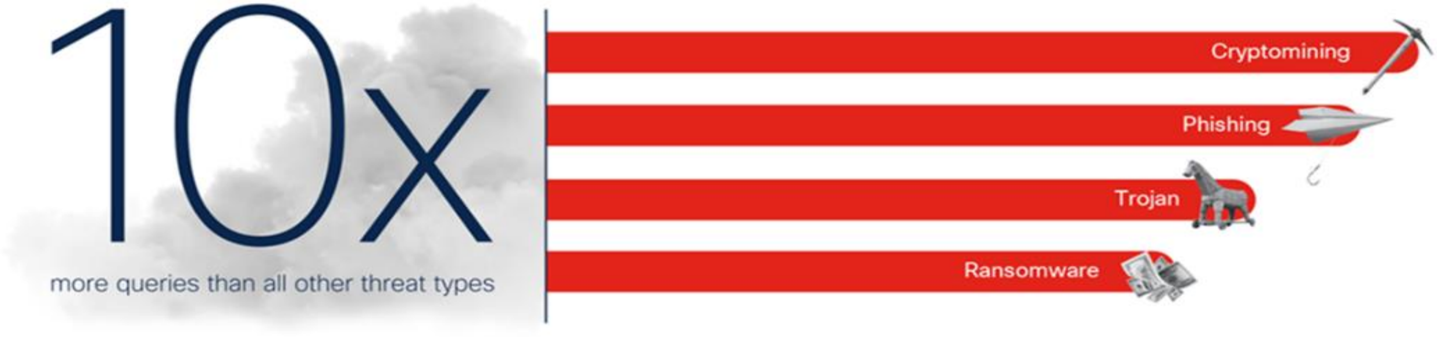
Amplified National Security Risk

Ransomware is becoming a national security risk, amplifying US Government focus given that organizations executing ransomware attacks may be state-sponsored, stemming from countries such as Russia, China, Iran, and North Korea, and given that recent attacks on critical infrastructure (i.e., Colonial Pipeline) and supply chain (i.e., Kaseya) demonstrate the potential for nationwide destruction.

Increasingly Profitable for Attackers

The economic incentive for ransomware attacks continue to grow as profits from past attacks fuel confidence for future attacks and the funding required to conduct them. The use of cryptocurrencies as a means to move ransom payments to jurisdictions without extradition treaties, combined with the difficulty to trace and recover funds, creates significant challenges for law enforcement.

Record-breaking year for data compromises and ransomware



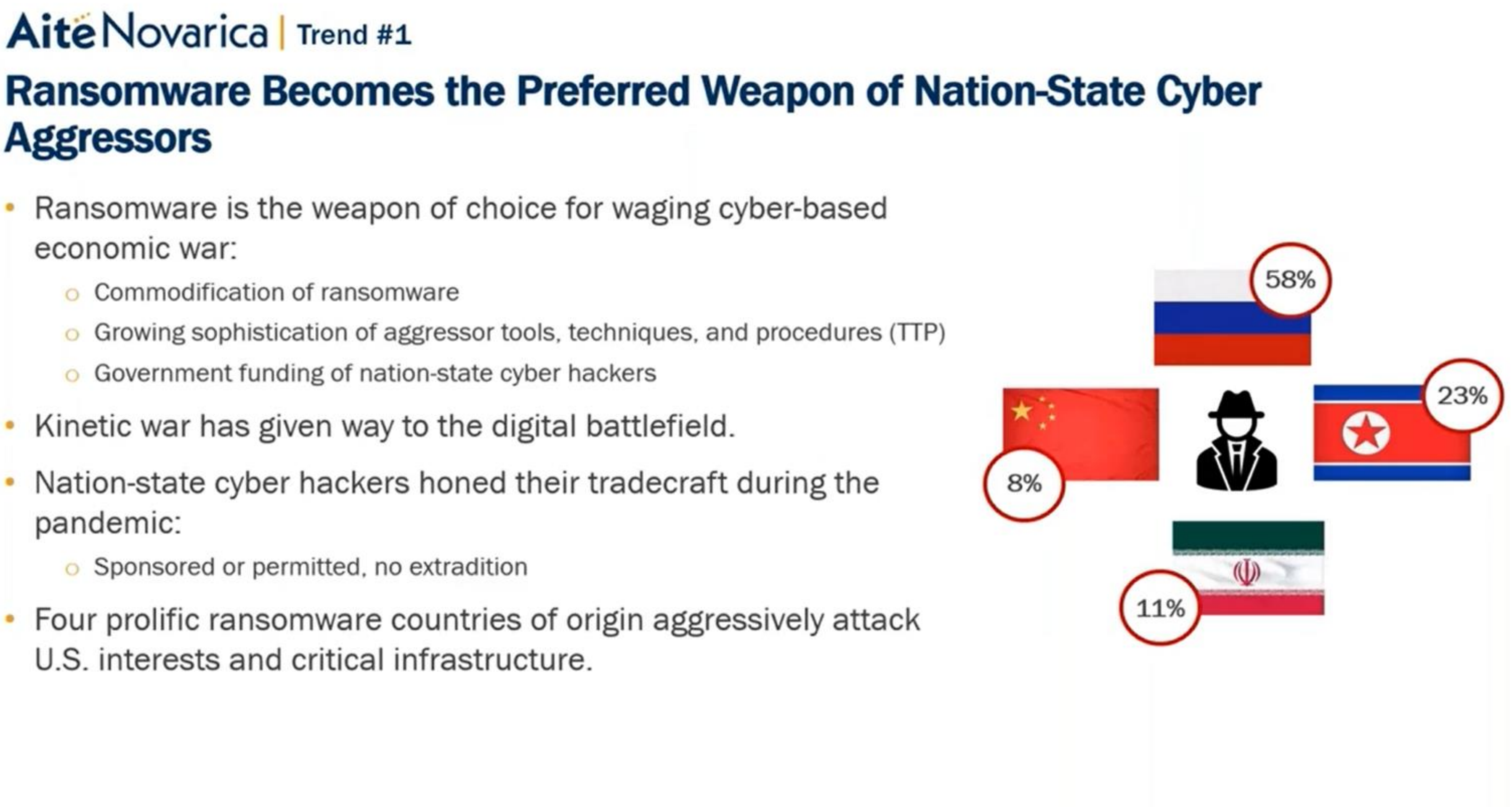
Source: CISCO’s 2021 Cyber security threat trends

“In 2021, cyber criminals executed a legion of highly coordinated, multi-step attacks”

- **86%** of organizations had at least one user try to connect to a phishing site
- **70%** of organizations had users that were served malicious browser ads
- **50%** of organizations encountered ransomware-related activity
- **48%** found information stealing malware activity

bpi
BITS

Record-breaking year for data compromises and ransomware



AiteNovarica | Trend #1

Ransomware Becomes the Preferred Weapon of Nation-State Cyber Aggressors

- Ransomware is the weapon of choice for waging cyber-based economic war:
  - Commodification of ransomware
  - Growing sophistication of aggressor tools, techniques, and procedures (TTP)
  - Government funding of nation-state cyber hackers
- Kinetic war has given way to the digital battlefield.
- Nation-state cyber hackers honed their tradecraft during the pandemic:
  - Sponsored or permitted, no extradition
- Four prolific ransomware countries of origin aggressively attack U.S. interests and critical infrastructure.

Ransomware – Prevention & Response Practices

Prevention Best Practices

- Maintain offline, encrypted backups of data and regularly test backups
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident
- Implement an awareness and training program that includes guidance on how to identify and report suspicious activity
- Conduct regular vulnerability scanning, patching and software updates
- Enable strong spam filters to prevent phishing emails from reaching end users and authenticate inbound email; scan all incoming and outgoing emails to detect threats
- Ensure devices are properly configured and security features are enabled
- Configure access controls with least privilege in mind
- Employ multifactor authentication for all services to the extent possible
- Employ best practices for use of Remote Desktop Protocol; consider disabling RDP if not being used
- Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB
- Consider the risk management and cyber hygiene practices of third parties and managed service providers; understand that adversaries may exploit the trusted relationships your firm has with third parties and service providers

"Let me be clear. Ransomware now poses a national security threat… cyber threats are coming dangerously close to threatening our lives."
- DHS Secretary Alejandro Mayorkas, March 31, 2021

What to do if infected with ransomware?

- Determine which systems were impacted, and immediately isolate them
- In the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection
- Contact law enforcement (the US Government strongly encourages firms to contact the FBI or Secret Service immediately upon discovery of a ransomware incident)
- Triage impacted systems for restoration and recovery, utilizing security incident response and business continuity plans
    - Identify and prioritize critical systems
    - Confirm nature of data impacted

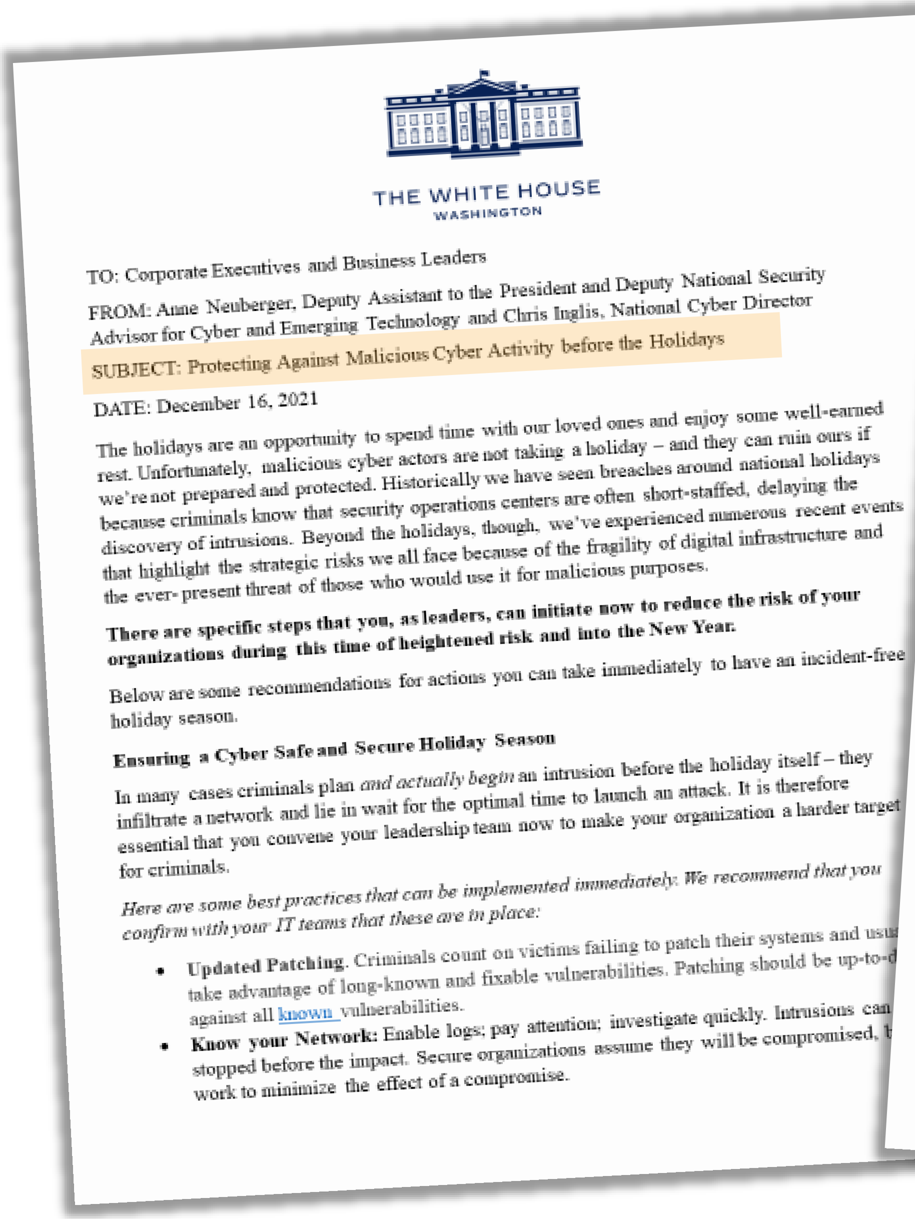
Should I pay a ransom?

- The FBI does not advocate paying a ransom because (1) it does not guarantee an organization with regain access to its data and (2) paying ransoms emboldens criminals.

"We recognize that victims of cyberattacks often face a very difficult situation and they have to just balance often the cost-benefit when they have no choice with regards to paying a ransom."
- Anne Neuberger, Deputy National Security Advisory for Cyber & Emerging Technologies, in response to the Colonial Pipeline outage

Sources: FBI's Internet Crime Compliant Center (IC3), CISA, Department of Justice, FinCEN, BPI's Ransomware Guide

White House Communications



THE WHITE HOUSE
WASHINGTON

TO: Corporate Executives and Business Leaders

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology and Chris Inglis, National Cyber Director

SUBJECT: Protecting Against Malicious Cyber Activity before the Holidays

DATE: December 16, 2021

The holidays are an opportunity to spend time with our loved ones and enjoy some well-earned rest. Unfortunately, malicious cyber actors are not taking a holiday – and they can ruin ours if we're not prepared and protected. Historically we have seen breaches around national holidays because criminals know that security operations centers are often short-staffed, delaying the discovery of intrusions. Beyond the holidays, though, we've experienced numerous recent events that highlight the strategic risks we all face because of the fragility of digital infrastructure and the ever- present threat of those who would use it for malicious purposes.

There are specific steps that you, as leaders, can initiate now to reduce the risk of your organizations during this time of heightened risk and into the New Year.

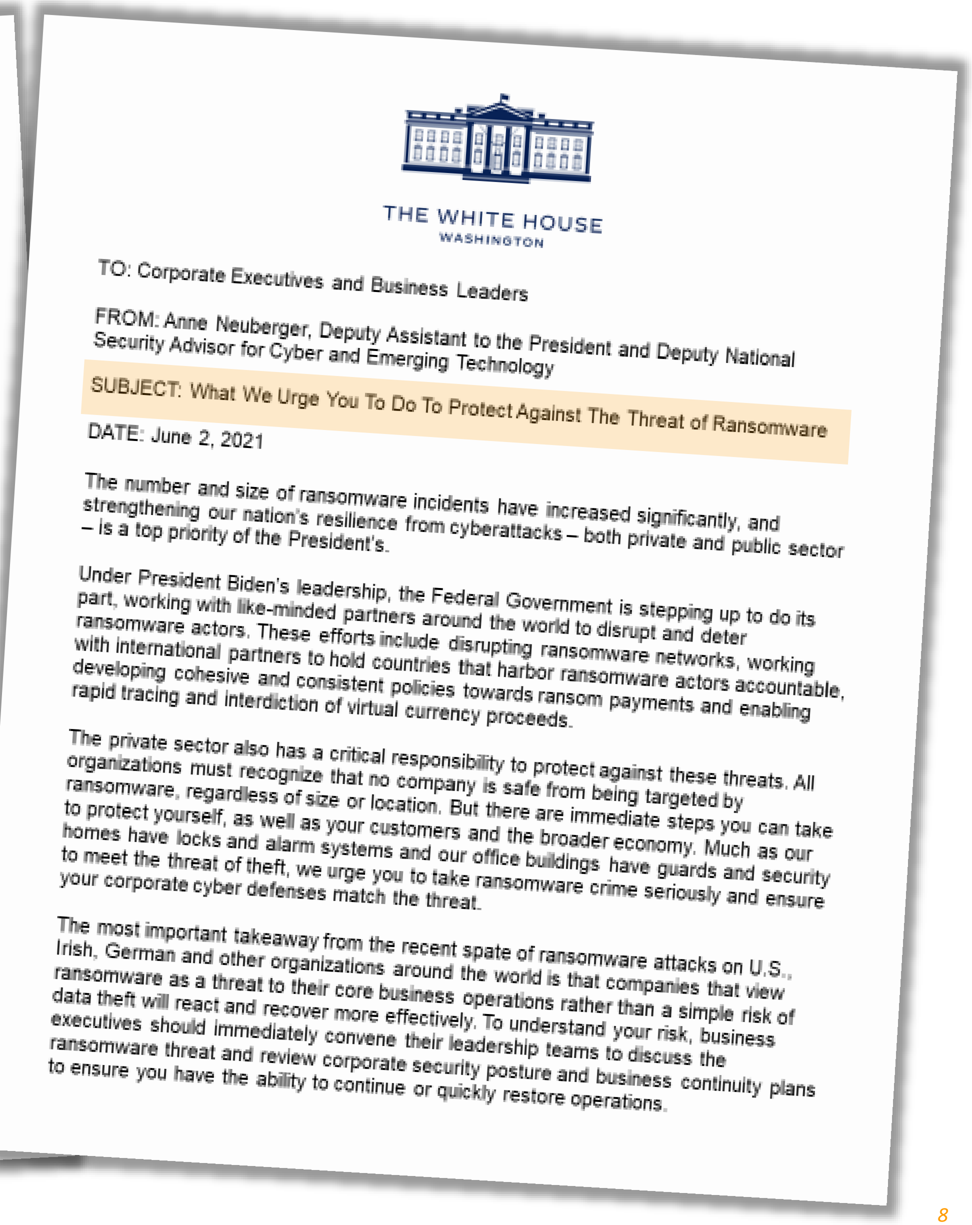
Below are some recommendations for actions you can take immediately to have an incident-free holiday season.

Ensuring a Cyber Safe and Secure Holiday Season

In many cases criminals plan *and actually begin* an intrusion before the holiday itself – they infiltrate a network and lie in wait for the optimal time to launch an attack. It is therefore essential that you convene your leadership team now to make your organization a harder target for criminals.

Here are some best practices that can be implemented immediately. We recommend that you confirm with your IT teams that these are in place:

- **Updated Patching.** Criminals count on victims failing to patch their systems and usu take advantage of long-known and fixable vulnerabilities. Patching should be up-to-d against all known vulnerabilities.
- **Know your Network:** Enable logs; pay attention; investigate quickly. Intrusions can stopped before the impact. Secure organizations assume they will be compromised, b work to minimize the effect of a compromise.



THE WHITE HOUSE
WASHINGTON

TO: Corporate Executives and Business Leaders

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

SUBJECT: What We Urge You To Do To Protect Against The Threat of Ransomware

DATE: June 2, 2021

The number and size of ransomware incidents have increased significantly, and strengthening our nation's resilience from cyberattacks – both private and public sector – is a top priority of the President's.

Under President Biden's leadership, the Federal Government is stepping up to do its part, working with like-minded partners around the world to disrupt and deter ransomware actors. These efforts include disrupting ransomware networks, working with international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds.

The private sector also has a critical responsibility to protect against these threats. All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location. But there are immediate steps you can take to protect yourself, as well as your customers and the broader economy. Much as our homes have locks and alarm systems and our office buildings have guards and security to meet the threat of theft, we urge you to take ransomware crime seriously and ensure your corporate cyber defenses match the threat.

The most important takeaway from the recent spate of ransomware attacks on U.S., Irish, German and other organizations around the world is that companies that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively. To understand your risk, business executives should immediately convene their leadership teams to discuss the ransomware threat and review corporate security posture and business continuity plans to ensure you have the ability to continue or quickly restore operations.

From DHS/CISA:

5 Questions CEOs Should Ask About Cyber Risks

1) What is the current level and business impact of cyber risks to our company? What is our plan to address identified risks?

2) How is our executive leadership informed about the current level and business impact of cyber risks to our company?

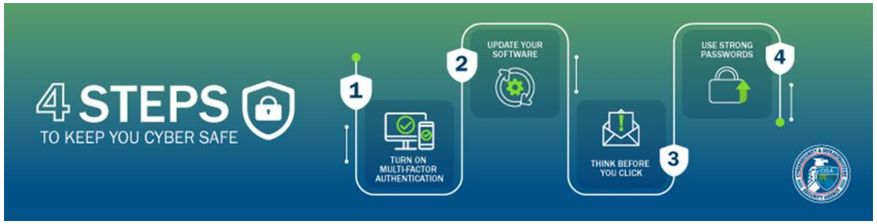
3) How does our cybersecurity program apply industry standards and best practices?

4) How many and what types of cyber incidents do we detect in a normal week? What is the threshold for notifying our executive leadership?

5) How comprehensive is our cyber incident response plan? How often is the plan tested?

…And 5 Tips to Get Your Organization Cyber Safe Today

TIP #1 STRONG CYBERSECURITY STARTS WITH CYBER HYGENIE



TIP #2 DEVELOP AND IMPLEMENT AN INCIDENT RESPONSE PLAN

TIP #3 PLAN, IMPLEMENT, AND TEST A DATA BACKUP AND RESTORATION STRATEGY

TIP #4 MAINTAIN AN EMERGENCY CONTACT LIST

TIP #5 REPORT THE COMPROMISE EARLY

Homepage | CISA