The Different Types of Cyber-Attacks Being Waged Today

We are in a true cyber war. This last year America had a 423 percent increase in hacks on financial firms alone! For this week's briefing, cyber and tech expert Robert Douglas is in the Economic War Room® to discuss the different types of cyber-attacks being waged today.

Cyber warfare is targeting the government, our infrastructure, financial institutions, and your money! This briefing provides an overview of what businesses and individuals should consider doing to better guard their information and money.

Your Mission: **To better protect your home, your finances, your business, or your employer from cyber-attacks.**

Ep. 4-151 (OSINT) Open-Sourced Intelligence Special Report. This includes conversations with Kevin Freeman and Robert Douglas

Robert is the founder and president of PlanetMagpie. Robert started his IT career as a programmer in 1984 and evolved into an expert network engineer specializing in Microsoft solutions. He has led consultant teams on projects for many of the world's major IT players including Microsoft, and leads PlanetMagpie's IT Consulting Team in a full range of network and cloud projects.

A respected IT expert in Silicon Valley, Robert has been quoted in the New York Times, CNN Money, Fast Company, the San Jose Business Journal, and the San Francisco Business Times. He also helped write Microsoft's Skype for Business Server certification exams for engineers. Originally from New York, Mr. Douglas received his B.S. in Computer Science from York College, and studied for his MBA at Union College.

1. **America is in a cyber war and it is impacting you!**
   Warning: We have had a 423% increase in hacks on financial firms this year.

   - The Cyber war has been going on for a while and it will never end!
   - Examples of countries that are hacking the US include China, Russia, Germany, Israel, and Iran.
   - Cyber attacks are a constant battle and will continue to be so in the digital world.
   - The US also does its fair share of hacking with other nations and has its own server farms.

   Not surprisingly it is the Democracies tend to be the primary targets of bad actors.
   The top four victims of hacking are:

   → America
   → United Kingdom
   → India
   → Germany

> "A cyber threat that scares me concerns the wanton destruction we would experience if a nation state took down our power grid, and everything is shut down." -Kevin Freeman

2. **A look at common cyber attacks and how they are implemented.**

   - The typical government vs government cyber-attack is a **denial of service.**
   - Another attack would be **the malware attack** to ruin the governments network or gather information on things they are doing.
   - Companies also face denial of service, but the big attack for companies is **phishing and spear phishing.**

⚠ WARNING: WATCH FOR THESE TYPES OF PHISHING ATTACKS

Spear Phishing Examples
"Let's say I work for you, you're my CFO, and somehow they've phished me and they figure out emails and whatnot. They've gotten into my contact list, now they send me an email from Kevin Freeman and say, 'Robert, it's Kevin. I have this big deal going on. I need you to transfer this amount of cash to this account and you give me the routing numbers and everything.' You would not believe how many companies fall for that. " –Robert Douglas

Other common hacks include:

- For financial advisors, it is, "Hey, I'm your client. I've got five hundred thousand dollars invested with you, but I got trapped in Europe."
- Also, you might get an email saying that there has been a compromise and you need to change your password. The forms looks official and they make you put in your email and previous password and steal that info.

"There's intellectual property ransom, which is paid in the form of Bitcoin, state and military secrets, blackmail, and personal information; which are your credit cards, your address, your Social Security numbers. Also, some of it's just mischief. We call them Kitty Scripters. There they go out, they find scripts, they run them just to see what they can do. And it causes lots of damage for private companies." –Robert Douglas

Cisco Systems defines Phishing this way and provides further insights of what to watch for: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

What is phishing?

Phishing attacks are counterfeit communications that appear to come from a trustworthy source, but which can compromise all types of data sources. Attacks can facilitate access to your online accounts and personal data, obtain permissions to modify and compromise connected systems--such as point of sale terminals

and order processing systems--and in some cases hijack entire computer networks until a ransom fee is delivered.

Sometimes hackers are satisfied with getting your personal data and credit card information for financial gain. In other cases, phishing emails are sent to gather employee login information or other details for use in more malicious attacks against a few individuals or a specific company. Phishing is a type of cyber-attack that everyone should learn about in order to protect themselves and ensure email security throughout an organization.

How does phishing work?

Phishing starts with a fraudulent email or other communication designed to lure a victim. The message is made to look as though it comes from a trusted sender. If it fools the victim, he or she is coaxed into providing confidential information--often on a scam website. Sometimes malware is also downloaded onto the target's computer.

Cyber-criminals start by identifying a group of individuals they want to target. Then they create email and text messages that appear to be legitimate but actually contain dangerous links, attachments, or lures that trick their targets into taking an unknown, risky action. In brief:

- Phishers frequently use emotions like fear, curiosity, urgency, and greed to compel recipients to open attachments or click on links.
- Phishing attacks are designed to appear to come from legitimate companies and individuals.
- Cyber-criminals are continuously innovating and becoming more and more sophisticated.
- It only takes one successful phishing attack to compromise your network and steal your data, which is why it is always important to Think Before You Click.

3. Beware of the Seven Key Attack Vectors in Cyber Warfare

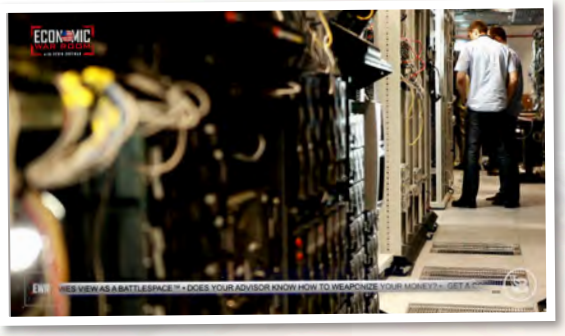
1. The first vector is the hardware itself.

- These are things like Wi-Fi routers, firewalls, and switches.
- Its best to have the top equipment for your safety. This includes companies like Juniper, F5, Cisco, and Extreme Switching. These are not typically consumer electronic purchases, but business applications.
- F5 is the only one that fully builds and designs in the US.

- Planet Magpie uses Juniper and Extreme on the inside of the network but uses F5 on the perimeter.

Even supposed US made equipment can be corrupted or counterfeit items made to look like US components.

"When I was working with the FBI on something, there were a bunch of 'Cisco' routers uncovered that when you looked at them, they looked perfectly normal. But when you dug down into them, there were mistakes inside the circuitry. They were counterfeit and I think they were from China." –Kevin Freeman



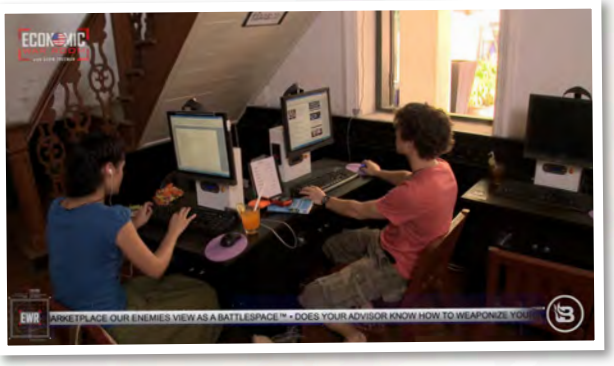
Note: Companies need to get better at their sourcing as that can create risk that they are not even aware of. A bad router from China could bring havoc.

- If companies are having their equipment manufactured in China, there is the concern that China will use that opportunity to steal information.

One of our biggest concerns right now, is all of our U.S. manufacturers, except for one, have their equipment manufactured in China. Now, the only one that I know of that completes their full build designs and everything here in the US is F-5." –Robert Douglas

2. The next vector is workstations.

- The workstation is things like laptops, desktops, iPads, and tablets.
- There needs to be a regimen where every month everything updates firmware, software, everything. Updates should be pushed out.
- Make sure everything is updated so that you decrease your risk of cyber-attacks.



3. The third vector is email.

- Email is one of the big entry points for hackers to come into your network.
- If one employee clicks one rogue message, then the network is locked up.
- Examples of this are phishing and spear phishing which was covered earlier.
- Segregation on machines is also important. You might not want to pay bills from the same computer that you read emails and surf the web.

"You know, I heard about a property tax assessor collector office where one employee clicked on a message, a birthday message, and it was supposed to be a photo. The next thing you know, they've lost $80 million." –Kevin Freeman

NOTE: In this case it would have been wise to have segregated the computers. One set of computers that accept and transfer funds, and separate computers that the employees use for email.

4. Cloud services - Another vector in cyber warfare is cloud services.

- Hackers will also target cloud services like Google Mail, Office 365, and other SAS.
- It always looks like an official email from one of these companies

An example in this case you might get a call. It's from someone **claiming** to be Microsoft or Apple Support calling to help. It is surprising how many people give up their credit cards. Sadly, they not only do they give up their credit cards, but cyber thieves also log on to your machine and they start copying files.

5. Servers are where the guts of the network live. They are the castles we want to protect.

- **Cyber warfare is targeted directly at the servers.**
- **Servers should be hardened to do only what they are designed to do.**
- **Servers should be locked down to individuals by department. That limits hacker access when there is an outbreak.**

"With servers we do a process called hardening. Hardening means that server can only do the functions it was meant to do. If it was a file server, it doesn't have a web server on it and it doesn't have ports open to the outside world." –Robert Douglas

6. Mobile devices are also an entry point to your information.
Cell phones may have access to a server and they need to be managed as well.

- To protect mobile devices, companies that require phones should purchase the phones for their employees so companies can manage the devices.
- IT companies can manage what's on the phones through what is called mobile device management.
- With mobile device management the phone it can be protected, if a phone is lost, information is scratched, all the data on it can be killed and company secrets protected.

7. The last vector is the Internet.

- The Internet is the access point for cyber. It could be your website being hacked or your WI-FI.
- It is important to protect employees from themselves through streamlining so that they cannot get to a bad site. Companies need to filter dangerous sites like porn and gambling sites that are compromised in order to reduce the threat of attacks from the Internet.
- Once a bad site gets in, a payload is put on your machine, and you will have ransomware.

4. Quick cyber tips you should consider for the home and office.

At minimum for home users, you should have a good firewall.

» Every home should have a good quality firewall. Businesses will require even more protection.

Businesses need to do even more.

» Businesses, both small and large, should make sure to get a more expensive firewall like a Juniper.

» Make sure your company considers cyber insurance.

» When looking for an I.T. consulting firm for your business, make sure they have the right solutions to building or reviewing an existing network. If they come back with things that you could buy off the shelf at a retailer, you have the wrong I.T. consultant.

- Also make sure to set up a plan for how often you update the firmware in order to protect your business.
- Network security needs to be a permanent fixture in every company's line budget.

5. **What can we do about the cyber threats? Stay alert and think before you click.**

   There are more cyber risk as more people work from home:
   - COVID-19 gave hackers a lot more opportunities to get into systems.
   - With more people working from home, there is less regulation and fewer IT standards in place.
   - Hackers also preyed on people searching the Internet for information on the COVID-19 virus.

6. **NSIC advisors will be encouraged to look at investment opportunities that help protect against cyber-attacks.**

   - As we look to protect our national security and economic infrastructure remember it is the democracies that are being attacked the most by bad actors.
   - Invest in and support cyber security companies that do their manufacturing in the U.S.
     → Robert Douglas suggested that one example of a cyber security company to consider investing in would be F5. They have some new components to their security that deal with bots and are focused on integrated US manufacturing.

   - Make sure your financial advisor is compliant and aware.
     → Financial advisors are under enormous scrutiny from the state securities agencies or the SEC to make sure they maintain a proper level of cyber-security. Still, it's good to ask what protections our advisor has in place.

     → Recognize the threat is much higher than it was in the past because everything is more connected.

7. **Despite all the cyber threats there are benefits of technology**
   - The free flow of information in this new age has helped both science and medicine, as well as businesses.
   - We have everything at our fingertips!
   - Technology can be a blessing and a curse.

- Big Tech is now working to censor people just like the Chinese Communist Party has done. The good news for America is that we are a free market, so new companies will grow and challenge big tech.

Why You Should Care:

- A wrong click can wreak havoc on your information and your money.
- Having a cyber plan for your business and home is important. Attacks are happening all the time and will continue.
- US manufacturing for IT components may be more important than many realize when it comes to cyber threats.
- Made in the USA, sometimes just means a product was assembled in the USA using Chinese or other adversary components.

Action Steps:

1. For your home network consider installing a quality firewall.
2. Always suspect Phishing as a possibility as you go through your emails.
3. Make sure your financial advisor is cyber compliant with their practice.
4. If you operate a business be sure to have a cyber-support team in place now, it will cost you more later if you don't.
5. If you operate a business you may want to consider purchasing cyber insurance to help protect from Internet-based risks and other risks related to information technology infrastructure, information privacy and information governance liability.
6. Individuals may want to consider joining an Identity Theft monitoring company.
7. Businesses may want to reach out to PlanetMagpie.com for a cyber audit.
8. Cyber threats are part of the economic war being waged against America and will continue. Fight back by weaponizing your money with investments that help support our national security and economic infrastructure.
9. **It is time to fight the economic war we are facing. Nominate your financial advisor at EconomicWarRoom.com/advisor** and let them know you think this would be a great opportunity for them. Classes are launching soon, and our list is growing fast.

10. Also, if you have not already done so, please consider the following:

Be sure to sign up for our free weekly Economic Battle Plans™ at www.EconomicWarRoom.com

- If you are following Economic War Room you will be on the leading edge as it relates to global threats, geopolitical analysis, and how you can weaponize your money to strengthen America. Your money, livelihood, and way of life are at risk and these tools are designed to mobilize America to protect their economic liberty.

In the **Economic War Room®**, we encourage Americans to be the "small ships that make the difference." You cannot solely rely on the government or the president to solve America's problems. You have to make a difference. It is up to you to help take our country back and create a voice for economic liberty. [The small ships are based on Churchill's Operation Dynamo that rescued the British Expeditionary Forces in the Miracle of Dunkirk.

We need more Economic Patriots on the team! Consider what you can do now to help strengthen America or even help someone in need. Keep in touch with your congressional representatives. Choose from the list or set your own goals:

√ At our Economic War Room® website, sign up to BlazeTV or LiftableTV for our complete weekly shows. Please use our code (**ECON**) from that link for a discount and FREE trial.

√ Follow, like, comment, and share on FB and Twitter. Look for short video segments on FB and Rumble and make sure. We recognize these tools may be compromised at times, but if they are not filtered, they are the major platforms available to reach out to the public. [Know that alternatives to the social platforms listed above are under EWR consideration.]

√ Check out XOTV (https://xotv.me/channels/233-economic-war-room), a new free speech video platform that Economic War Room is proud to partner with. Access is FREE but consider making a donation to EWR on that website to help with Economic War Room's research and production costs.

√ You are welcome to share this Economic Battle Plan™ and our short video segments with friends on FB or YouTube. We set up the Economic War Room® to be your resource for information, preparation, and mobilization.

√ Do this now! Have a financial action plan based on multiple geopolitical scenarios developed now. Advanced preparation is key. Trying to figure what to do when an economic event happens is usually too late.

Shareable Quote:

"Think before you click."

– CiscoSystems

The EWR Collection Deck – From Kevin Freeman

(List of resources and external links for more information)

Quick Access Links

[ ] - Must Read/Watch

Where to Access Economic War Room

On BlazeTV https://get.blazetv.com/economic-war-room/
On LiftableTV https://liftable.tv/economicwarroom/
XOTV Channel https://xotv.me/channels/233-economic-war-room
Website https://www.economicwarroom.com/
TUVU (download the app on the iTunes or Andriod Store) **follow us @EconomicWarRoom**
Facebook page https://www.facebook.com/economicwarroom/
Twitter page https://twitter.com/economicwarroom
YouTube page https://www.youtube.com/economicwarroomwithkevinfreeman
Rumble page https://rumble.com/c/c-408647
Parler page https://parler.com/profile/EconomicWarRoom/posts
Gettr page https://gettr.com **follow us @economicwarroom**
Link to all Economic Battle Plans™ https://www.economicwarroom.com/battleplans

Episodes and Economic Battle Plans™ from Prior Shows with Application to this Topic:

[ ] 06/24/21, EP144, **IMPORTANT!** All Enemies Foreign and Domestic, Download Economic Battle Plan™
[ ] 01/21/21, EP122, China Special Part 2, Dave Brat, Eric Bolling, Download Economic Battle Plan™
[ ] 01/07/21, EP120, China Special Part 1, Gordon Chang & Rod Martin, Download Economic Battle Plan™
[ ] 12/17/20, EP118, Rise of the Machines, Download Economic Battle Plan™
[ ] 09/17/20, EP105, **IMPORTANT!** China's Unrestricted Warfare, Download Economic Battle Plan™
[ ] 07/23/20, EP97, China's Stealth War, Gen. Spalding, Download Economic Battle Plan™

[ ] 01/23/20, EP70 Our Elections Can Be Hacked - **CRITICAL DOWNLOAD**, Download Economic Battle Plan™
[ ] 10/17/19, EP57 Brig. Gen Robert Spalding (ret), Download Economic Battle Plan™
[ ] 09/12/19, EP52 Brig. General Robert Spalding-CHINA, Download Economic Battle Plan™
[ ] 01/24/19, EP18 Personal CYBER threats and safety, Download Economic Battle Plan™
[ ] 10/11/18, EP02 Democrat IT Scandal, Download Economic Battle Plan™

About Robert Douglas and Planet Magpie

[ ] Planet Magpie https://planetmagpie.com/about/why-choose-us

[ ] Planet Magpie Data Sheets https://planetmagpie.com/about/downloads#datasheets

Services Overview
https://planetmagpie.com/docs/default-source/downloads/datasheets/servicesoverview2018web0db561ec43ca6e2c9869ff00006b8bbb.pdf?sfvrsn=e8420e7b_7

7 Ways You Can Save on Your IT Costs Now
https://planetmagpie.com/docs/default-source/downloads/lead-magnets/7-ways-you-can-save-on-your-it-costs-right-nowb8b561ec43ca6e2c9869ff00006b8bbb.pdf?sfvrsn=589d0f7b_7

[ ] The Case for a Virtual CIO
https://planetmagpie.com/docs/default-source/downloads/white-papers/planetmagpie-white-paper---the-case-for-the-virtual-cio.pdf?sfvrsn=9e480e7b_16

Keeping Strawberries Safe: PlanetMagpie Builds Event Management Application to Track Strawberry Grower Safety Training
https://planetmagpie.com/docs/default-source/downloads/case-studies/pm_csc-sitefinity_casestudy-02012013.pdf?sfvrsn=fba9307b_2

Are You Still Making these Basic Email Privacy Mistakes?
https://www.fastcompany.com/3050656/why-are-you-still-making-these-basic-email-privacy-mistakes

Alpha Dog (Robert Douglas) https://planetmagpie.com/about/team-leads

Foreign Cyber Threats

[ ] China has stolen enough data to compile a 'dossier' on every American
https://news.yahoo.com/china-stolen-enough-data-compile-110000433.html

US Charges 4 Chinese Nationals Working With Spy Agency in Global Hacking Campaign
https://theepochtimes.com/mkt_morningbrief/us-condemns-chinas-malicious-cyber-hacking-says-china-behind-microsoft-hack_3907751.html

[ ] Can We Talk About Joe Biden's Horrible Choice to Give Putin a List of Things Not to Cyberattack?
https://pjmedia.com/news-and-politics/bryan-preston/2021/06/17/can-we-talk-about-joe-bidens-horrible-choice-to-give-putin-a-list-of-things-not-to-cyberattack-n1455346

The Ransomware Problem Shows That Russia Is Either a Rogue State or a Failed State
https://thebulwark.com/the-ransomeware-problem-shows-that-russia-is-either-a-rogue-state-or-a-failed-state/

China-Linked Hack Hits Tens of Thousands of U.S. Microsoft Customers
https://www.wsj.com/articles/china-linked-hack-hits-tens-of-thousands-of-u-s-microsoft-customers-11615007991

[ ] Hack of Federal Government Larger Than Previously Thought, Warns CISA
https://www.theepochtimes.com/hack-of-federal-government-larger-than-previously-thought-warns-cisa_3623466.html

Four Members of China's Military Indicted Over Massive Equifax Breach
https://www.wsj.com/articles/four-members-of-china-s-military-indicted-for-massive-equifax-breach-11581346824

Russian Hackers Continue With Attacks Despite Biden Warning
https://www.bloomberg.com/news/articles/2021-07-30/russian-hackers-continue-with-attacks-despite-biden-warning

Russian hackers target aid groups in new cyber-attack, says Microsoft
https://www.bbc.com/news/world-us-canada-57280510

Facebook Warning: U.S. Military Targeted By Iranian Hackers Posing As Attractive Women
https://www.forbes.com/sites/thomasbrewster/2021/07/15/facebook-iranian-fakes-hack-us-military/

State-Sponsored Iranian Hackers Indicted for Computer Intrusions at U.S. Satellite Companies
https://www.justice.gov/opa/pr/state-sponsored-iranian-hackers-indicted-computer-intrusions-us-satellite-companies

Publicly Reported Iranian Cyber Actions in 2019
https://www.csis.org/programs/technology-policy-program/publicly-reported-iranian-cyber-actions-2019

[ ] The Incredible Rise of North Korea's Hacking Army
https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army

North Korean hackers are 'the world's leading bank robbers,' U.S. charges
https://www.politico.com/news/2021/02/17/us-charges-north-korean-hackers-wannacry-sony-469406

U.S. accuses three North Koreans of conspiring to steal more than $1.3 billion in cash and cryptocurrency
https://www.washingtonpost.com/national-security/north-korea-hackers-banks-theft/2021/02/17/3dccf0dc-7129-11eb-93be-c10813e358a2_story.html

[ ] Counterfeit Chinese Technology: Gateway for Hacker
https://abcnews.go.com/TheLaw/FedCrimes/story?id=4825112&page=1

Criminal Cyber Threats

Widespread ransomware attack likely hit 'thousands' of companies on eve of long weekend
https://www.washingtonpost.com/technology/2021/07/02/kaseya-ransomware-attack/

[ ] Significant Cyber Incident report
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Hackers Stole Nearly 26 Million User Login Credentials for Sites Like Amazon, Google, Facebook
https://theepochtimes.com/hackers-stole-nearly-26-million-user-login-credentials-for-sites-like-amazon-google-facebook_3855766.html

CNBC: Meat supplier JBS paid ransomware hackers $11 million
https://www.cnbc.com/2021/06/09/jbs-paid-11-million-in-response-to-ransomware-attack-.html

[ ] The Colonial pipeline ransomware hackers had a secret weapon: self-promoting cyber-security firms
https://www.technologyreview.com/2021/05/24/1025195/colonial-pipeline-ransomware-bitdefender/

'It's a battle, it's warfare': experts seek to defeat ransomware attackers
https://www.ft.com/content/b48a2d70-4a8c-4407-83a2-59cd055068f8

America under siege on Biden's watch as cyberattackers cripple the country
https://washingtonguardian.org/articles/america-under-siege-on-biden-s-watch-as-cyberattackers-cripple-the-country

Apple targeted in ransomware attack with files stolen from Mac Pro manufacturer
https://seekingalpha.com/news/3685028-apple-targeted-in-ransomware-attack-with-files-stolen-from-mac-pro-manufacturer

[ ] Beyond creepy: 150,000 security cameras hacked
https://www.wnd.com/2021/03/beyond-creepy-150000-security-cameras-hacked/

At least 10 hacking groups using Microsoft software flaw -researchers
https://news.trust.org/item/20210310152040-foj30

[ ] Florida Water Supply Hack Demonstrates Our Vulnerability to Cyberattacks
https://www.theorganicprepper.com/fl-water-hack-cyberattack/

The Year of the Hack: 5 of 2020's Biggest Security Breaches
https://www.breitbart.com/tech/2021/01/01/the-year-of-the-hack-5-of-2020s-biggest-security-breaches/

Hackers can now clone your keys just by listening to them with a smartphone
https://mashable.com/article/spikey-house-keys-listening-smartphone/

Massive spying on users of Google's Chrome shows new security weakness
https://www.cnbc.com/2020/06/18/massive-spying-on-users-of-googles-chrome-shows-new-security-weakness.html

CIA cyber weapons stolen in historic breach due to 'woefully lax security', internal report says
https://www.cnn.com/2020/06/16/politics/cia-wikileaks-vault-7-leak-report/index.html

[ ] Cisco partners sell fake routers to US military
https://www.zdnet.com/article/cisco-partners-sell-fake-routers-to-us-military/

The Anatomy of a Cisco Counterfeit Shows Its Dangerous Potential
https://www.wired.com/story/counterfeit-cisco-switch-teardown/

Responses and Mitigation Strategies

[ ] Cyberattacks Aren't Going Anywhere – We Need a National Strategy to Fight Them
https://townhall.com/columnists/carolinewang/2021/06/12/cyberattacks-arent-going-anywhere--we-need-a-national-strategy-to-fight-them-n2590797

Lawmakers Introduce Bill Allowing Americans to Sue Foreign Hackers in US Courts
https://theepochtimes.com/lawmakers-introduce-bill-allowing-americans-to-sue-foreign-hackers-in-us-courts_3725834.html

[ ] How to respond to Russia's SolarWinds cyberattack
https://www.aei.org/op-eds/how-to-respond-to-russias-solarwinds-cyberattack/

[ ] 6 Strategies for Cyber-security Risk Mitigation
https://securityscorecard.com/blog/6-strategies-for-cybersecurity-risk-mitigation

NSA'S Top Ten Cybersecurity Mitigation Strategies
https://www.nsa.gov/Portals/70/documents/what-we-do/cyber-security/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf

[ ] An Ongoing Project: A Cyber Risk Mitigation Strategy
https://www.getsmarter.com/blog/market-trends/an-ongoing-project-a-cyber-risk-mitigation-strategy/

The 7 attack entry points cyber-criminals look for and the best ways to defend them.
https://planetmagpie.com/news/woof-newsletter/2021/06/09/the-7-attack-entry-points-cybercriminals-look-for-(and-the-best-ways-to-defend-them)