Reframing the Risk Calculus for Insurance of Nation-State Cyber Attacks

CHRIS NISSEN

FOUNDER AND CEO, SOUHEGAN GROUP RISK SOLUTIONS

CHRIS NOLAN

VICE PRESIDENT OF MARKETING, INTANGIC

RYAN DODD

FOUNDER AND CEO, INTANGIC

Reframing the Risk Calculus for Insurance of Nation-State Cyber Attacks

MAY 19, 2023

Executive Summary

Outside of the individuals and entities fighting on the frontlines of cyber warfare today, the general perception of state-sponsored cyber adversaries' tactics and activities is different from the reality. Specifically, the fear of a rare, catastrophic 'Cyber Armageddon' event that could happen runs contrary to the constant stealth attacks that are happening and puts corporations and economies at risk of misallocating resources to effectively manage this dynamic threat. Recent developments like the Lloyd's of London *State backed cyber-attack exclusions requirement* for insurers represent a change in the legal framework for some market participants.[1] This paper will outline that solutions for companies do exist, including insurance. There is a business case for corporate leaders to address the risk more effectively.

This paper will argue that understanding of the frequency and severity of attacks and the tactics employed by nation-state adversaries can better protect against the more probable events that could cause economic damage to companies. If risk management programs put too much emphasis on planning for a rare Cyber Armageddon, we could end up creating a blind spot in containing losses from a much higher likelihood event risk: a less severe nation-state attack unintentionally causing a chain reaction of "cascading" damages.

It is true that cyber attacks have been growing at a tremendous pace for years now. Though criminal actors are a prime threat for any company, any of these events are in fact perpetrated by nation-state actors both directly and indirectly via state-backed criminal proxies executing ransomware attacks. However, these actors are careful to limit their effects to ensure they stay below the threshold of war. If the cyber insurance market withdraws from insuring these everyday, low severity attacks, the overall infrastructure may become increasingly fragile and may actually inadvertently work to help better position a nation-state across a wide swath of the private sector cyber landscape thus enabling a much larger, devastating attack in the future.

To encourage future discussion on this topic from an insurance and broader risk management perspective, we outline factors that our research suggests are a source of misperception of frequency and severity when corporations assess risk programs to protect against nation-state adversaries:

1. Lloyd's of London, Market Bulletin Ref Y5381. August 16, 2022.

1. Nation-state adversaries are skilled at emplacement and execution yet can be detected at various 'pre-event' stages. But if you can't see the threat, it's hard to believe it exists.

2. Companies have underinvested in detection vs. prevention technology due to how the adversary operates and the way the cybersecurity vendor and customer ecosystem has evolved in the past decade.

3. Western government efforts at cyber deterrence and retribution are working, and adversaries know there is a line not to be crossed when attacking economic and critical infrastructure that would trigger a response. In other words, the adversaries know how to carry out damaging attacks while staying below the threshold of war.

We will also examine the lasting impact of the adversaries' success with asymmetric warfare tactics that treat companies as legitimate strategic targets to steal valuable IP, disrupt operations, and weaken key economic interests. In examining state-actor risk from the adversary point of view (POV) versus the defender (and indeed the insurer POV), we can better understand the actual frequency, tactics and impact of this threat activity today. As a result, corporations and their insurers can apply stronger risk management strategies based on the state-actor threats happening every day versus preparing for a Cyber Armageddon that has not yet—and is unlikely to—materialize.

The size and scale of Chinese-backed attacks on corporate networks in 2022 increased significantly, targeting every major industry sector.[2]

Paradoxically, risk management approaches that over-emphasize a Cyber Armageddon event often lead to the belief that such an event is "unmanageable and undefendable", resulting in a dangerous complacency. If we decide we cannot manage the risk at all, we could actually increase the likelihood of one of these more frequent, less severe events cascading into a level of economic losses that insurers and companies are seeking to avoid with increasing policy exclusions for cyber war and state-actor attacks.

This perception blind spot is also likely to lead to a rising number of corporations that are under-protected and largely uninsured, posing a significant threat to economic interests and national security.

Defending against the mostly highly skilled cyber war attackers is a hard, dynamic problem outside the core risk expertise of most companies. However, by thinking differently about the risk, we can adjust our perception of the threat and better prevent the more frequent attacks from cascading into severe economic loss.

2. Crowdstrike. 2023 Global Threat Report. 2023. (https://www.crowdstrike.com/global-threat-report/)

This paper will demonstrate that there is a business case for a proactive approach by the insurance market and companies. A middle ground can exist between companies seeking to lower the amount of uninsured risk, and an insurance industry seeking to avoid too much exposure to a risk that is not well understood. It first requires a better understanding of the risk by all parties and a reallocation of resources towards measures that can increase resilience.

In the process, we aim to dispel three misconceptions and illustrate how corporate risk management programs can better offset nation-state cyber attacks. While the cyber protection gap remains significant for reasons beyond nation-state risk, we believe that addressing these issues can help reduce their overall loss exposure due to cyber.

Perception	Reality
Nation-state attacks are most likely to be a catastrophic, rare 'Cyber- Armageddon' event.	Nation-state cyber attacks are much more common than most realize due to an 'asymmetric' shift in the threat environment, and skill of adversaries to carry out attacks largely undetected.
Nation-state attacks are indefensible and thus resources are best spent focused on criminal threats.	Many targets of nation-state actors are vulnerable enough that highly advanced techniques are not required. The' human domain' is a key, often overlooked, threat vector. A reallocation of resources towards more advanced threat detection is needed.
Accept that nation-state risk is a largely uninsurable risk 'you simply have to live with' and hope it doesn't materialize.	Thinking differently about the nation-state cyber risk helps remove the perception blind spot and opens up better risk transfer options that incentivize resilience to deal with risk as it is today, not as it is imagined.

Reality 1: In the era of asymmetric warfare, Nation-states are performing cyber attacks all the time vs. planning a big catastrophic event.

Nation-state attacks are much more common than most realize. Nation-state adversaries' interest in private sector companies is due to many factors including economic and traditional espionage, data theft, software supply chain penetration (infiltration of your system via a software injection vs a direct cyber attack), monetary gain, pre-positioning of capabilities (backdoors), as well to exert influence over sovereign governments through social disruption and exploitation of critical infrastructure, including transportation, healthcare, banking and other vital capabilities. There are numerous examples of attacks against the private sector in these areas by China, Russia, North Korea and others.

One reason C-suites perceive this risk as a low frequency, high severity event is because the threat actor's objective is to go undetected, and the attacks usually do. This is often because most systems are constructed largely for prevention. Less attention is paid to detection, and even less is paid to early detection in the attack cycle which can amount to a prediction of an attack. In a majority of attacks, the state actor's objective is surveillance and data gathering for the purposes of carrying out a more damaging attack later.[4] Recently, we have observed a shift in sophisticated ransomware groups in which these adversaries take time to quietly maneuver a network to identify the most critical data before deploying the ransomware. This further underscores the critical value of detection capabilities in a corporate cybersecurity program.

100% rise in 'significant' nation-state incidents between 2017-2020[3] and still no 'Cyber Armageddon'

Better understanding the state actor's behavior helps prepare for the 'what now' vs. 'what if'

Typical state actor behavior stands in contrast to a criminal cyber group's 'smash and grab' approach characterized by large scale data theft or a ransomware attack, although early cyber detection capabilities can be immensely useful for these as well.

Asymmetric Era

Companies are now operating in an Asymmetric Era[5] often without explicitly realizing it. This shift means companies' valuable assets and their impact on the economy are treated with increasing frequency as legitimate targets by nation-states.

Beginning around 1990, China and Russia pivoted to an asymmetric strategy against their adversaries. Key characteristics of this shift include:

1. Key adversaries of western countries no longer must engage through traditional 'kinetic' means to achieve their objectives. This means companies—the primary source of economic power—are treated as legitimate targets by 'non-kinetic' means—in the cyber, human, and supply chain domains, much more than they realize. In a rare admission, a senior Chinese military officer at a 2014 meeting in Washington stated: "**We don't draw the line between national security and economic espionage the way you do. Anything that builds our economy is good for our national security.**"[6]

3. Ibid.
4. Dr. Michael McGuire, Nation States, Cyber Conflict and the Web of Profit (HP and HP Wolf Security). 2021.
5. Christopher Nissen, John Gronager, PhD., Rober Metzger, J.D., Harvey Rishikof, J.D., "Deliver Uncompromised, A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War", August 2018.
6. Yudhijit Bhattacharjee, The Daring Ruse that Exposed China's Campaign to Steal American Secrets, The New York Times, March 2023.

2. Governments and companies have been slow to adapt to this new era, generally failing to think holistically about the risks.[7]

3. Companies that only focus on one of these domains, like cyber, as the primary vector for potential attack, afford nation-state adversaries greater opportunities to exploit the others (human/insider and supply chain including software, hardware, and service providers).

Since 1990, many other nation-states aside from China and Russia have followed suit with exploitation at-scale of all the elements of globalization in hundreds of verticals, including infrastructure, finance, logistics, transportation, and healthcare.

110% increase in ICS/OT vulnerabilities disclosed from 2018-2021 and 63% of which can be executed remotely.[8]

In recent years, Mandiant has observed a significant increase in threat activity with the potential to impact production for industrial and critical infrastructure organizations, including nation-state actors.[9]

Emergence of the Asymmetric Era

The result of the shift is businesses now carrying large operational risks via supply chain vectors: Cyber, Software/Hardware, Insiders, other 3rd Parties.

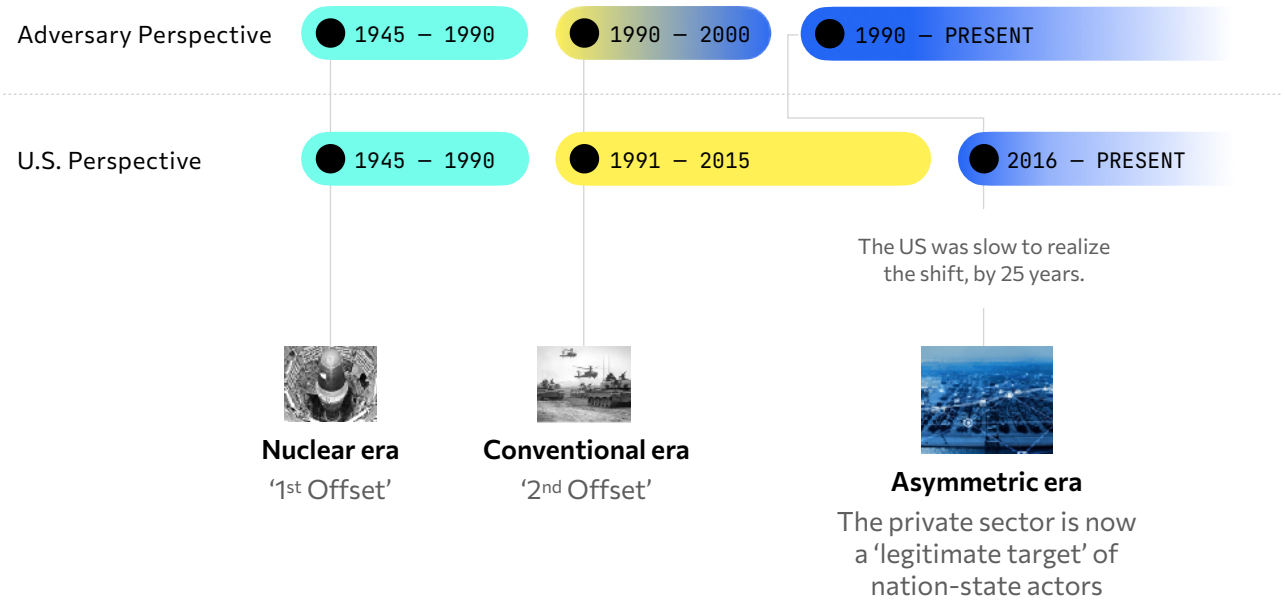


Figure 1. Emergence of Asymmetric Era

Source: Christopher Nissen, John Gronager, PhD., Rober Metzger, J.D., Harvey Rishikof, J.D., "Deliver Uncompromised, A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War", August 2018.

7. This happened for a variety of reasons including that many Western companies embraced globalization seeing opportunities for profit while our adversaries saw it as an opportunity to penetrate these companies. Beginning in the early 2000s, many companies including Microsoft were required to turn over their source code to the Chinese government for inspection as a condition for a license to operate. Recently China has demanded having CCP members on the board of companies with China-based operations.
8. Claroty Biannual ICS Risk and Vulnerability Report: 2H 2021
9. Mandiant. The Defenders Advantage Cyber Snapshot. (https://www.mandiant.com/media/16581)

Not only are there targeted attacks on precise organization-level vulnerabilities, but there are also tactics that leverage system-level dependencies that expose companies to risks arising from the reliance on extremely complicated supply chains. This includes cloud data storage, third-party processing and communications, and a broad range of rapidly-evolving and cost-effective new digital manufacturing and information technologies that are subject to destabilizing cycles of innovation. These attacks primarily exploit 3rd party trusted relationships, including a broad range of suppliers, contractors, employees and business relationships.

In other words, companies can no longer think about nation-state risk with the mindset that only critical infrastructure companies or those very close to them are at risk, or that government intervention is going to prevent or backstop the effects of such attacks. In fact, nearly all large companies are at risk because of what the Risk and Insurance Management Society ("RIMS") refers to in a paper responding to the Federal Insurance Office ("FIO") in the US as the 'cascading effect' on the "Potential Federal Insurance Response to Catastrophic Cyber Incidents". It describes how the failure of a primary system will cascade to multiple other system failures beyond the traditional scope of 'critical infrastructure'.[10] This is no doubt a legitimate concern for insurers and insureds alike.

Cascading Impact: Nation-State Asymmetric Targeting of Private Enterprise

While state actor behavior suggests a planned Cyber Armageddon attack is highly unlikely, we do believe these smaller more frequent state actor attacks could lead to a chain reaction of increasingly severe 'cascading events', which in aggregate could look like a Cyber Armageddon but would likely be an unintentional result of the attacker. Our aim is to place attention on strengthening corporate risk management programs with better detection and resilience that can minimize the likelihood of a cascading event in the first place.

A recent example of this cascading impact is the Viasat event in February 2022. In this case, the attack did not spread beyond second order cascading impact. Viasat, the communications technology company, announced a disruption to its network due to a cyber breach of its satellite internet system. The network disruption, originating in Ukraine but impacting the company's network in Europe and Ukraine, was believed to have been perpetrated by the Russian government or an affiliated group ahead of the Russian military's invasion—part of a military concept termed "preparing the battlefield". We observe this practice of cyber and supply-chain exploitations via the pre-positioning of tools for a timed future execution, once again underscoring the importance of early detection.

10. Mark Prysock, Comment Letter on Potential Federal Insurance Response to Catastrophic Cyber Incidents (The Risk Management Society). 2022. (https://rims.org/docs/default-source/default-document-library/advocacy/rims-fio-comment-letter-11-14-22.pdf?sfvrsn=68ab91d3_3)

Service disruptions for customers in Europe lasted over one month, and up to 3,000 wind turbines that relied on the network were disconnected in Germany. Remote monitoring and control of thousands of wind turbines failed according to Dominik Bertrams of wind farm operator Tobi Windenergie Verwaltungs GmbH.

Though it is unlikely the German wind operator was directly targeted in the attack, its reliance on a supply chain that was directly targeted by a nation-state adversely impacted its operations and customers.

Use Case — Cascading Impact: Asymmetric Targeting

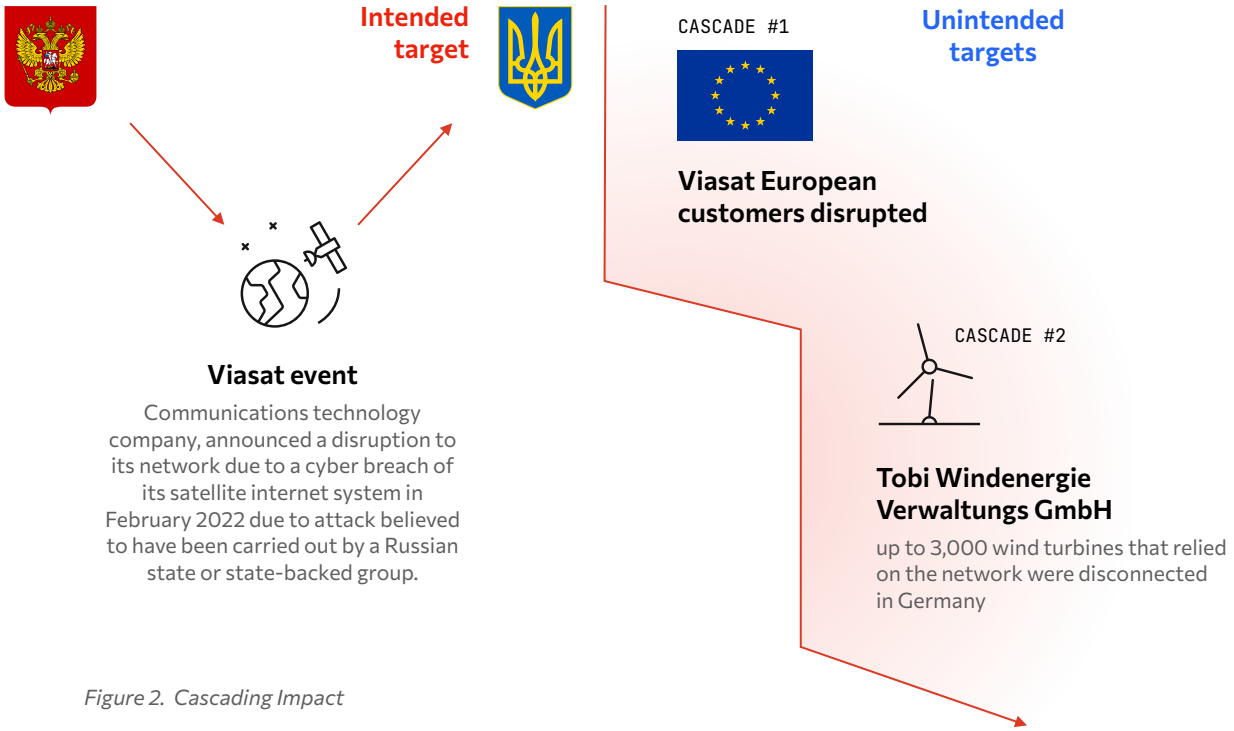


Figure 2. Cascading Impact

Although awareness of data breaches, ransomware, and sabotage events has grown along with the continued growth in spending on cybersecurity, what's missing is a system-level understanding of cyber, human and supply chain risk that links to effective risk strategies, including insurance.

In the asymmetric era, the supply chain is a key factor for triggering cascading events. Another way the nation-state actor behavior is not yet well understood is how they exploit an expanded spectrum of attack vectors across a corporation, including the formal supply chain. In other words, if companies are only looking at vulnerabilities in the cyber realm, they are missing a wider set of attack activity in other vectors.

High level 'Supply Chain' attack vectors

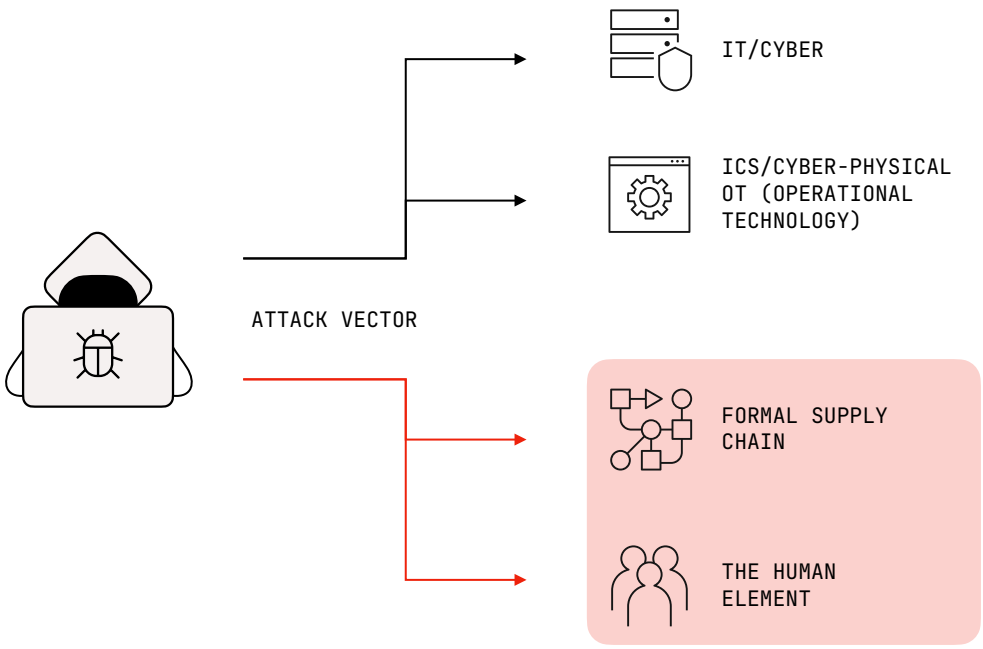


Figure 3. Supply Chain Threat

An enterprise's supply chain is basically the sum of its third-party risk. As the above graphic illustrates, the highest-level attack vectors are Cyber (IT & OT), formal supply chain (software, hardware, services), and the human domain (insider/outsider, witting, unwitting).

Most companies are indeed susceptible to a damaging third-party or insider risk—where a third-party supplier offers a service then breaches that trust and steals information through a range of tactics.[11] For example, law firms that specialize in patent filings on behalf of large corporate clients have been targets of nation-state actors for years.[12] Likewise, employees may unwittingly put the enterprise at risk through technical or programmatic communications for which they are being solicited.

Risks within the supply chain, including employees and employees of suppliers, are often a source of significant unknown risk for companies—both wittingly and unwittingly. The solution requires a holistic counter-intelligence approach based on a deep understanding of these vectors and the ever-changing techniques employed by the attacker.

11. US Department of Homeland Security, DHS Statement on the Issuance of Binding Operational Director 17-01. 2017. (https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01)
12. Ionut Arghire, Chinese Hackers Spy on U.S. Law Firm, Major Norwegian MSP (Security Week), 2019. (https://www.securityweek.com/chinese-hackers-spy-us-law-firm-major-norwegian-msp/)

The China Threat

The China threat involves all four attack vectors and highlights just how high frequency the state actor threat actually is for corporations. It used to be that companies outside of traditional critical infrastructure and defense sectors did not perceive themselves to be a target for Chinese state and state-sponsored threat groups. But the frequency with which the FBI is opening counter-intelligence cases against China involving US companies is just one indication that a far larger cross-section of companies is under constant threat from these groups.

Some context:

1. Made in China 2025, the Belt and Road Initiative, and numerous behaviors, statements, and actions by China, Russia and others over the past several years have illustrated their intent and capabilities against companies. In fact, in the new Asymmetric Era, hardly any industry vertical is immune from nation-state strategic targeting—either directly or indirectly - as part of a larger global economic warfare strategy.

2. The growing scale of the problem was highlighted by FBI Director Christopher Wray: "Over 2,000 open investigations are focused on the Chinese government trying to steal our information or technology—there is just no country that presents a broader threat to our ideas, our innovation, and our economic security than China." He added that the Bureau opens a new counter-intelligence case against China about twice a day."[13]

Most of these investigations capture only a fraction of actual threat activity from China. Potential losses stemming from threat activity like this materializes outside the public or even company eye.

This is a higher frequency dimension of the nation-state threat that does not shape common perceptions of the risk in the minds of most corporate leadership. This is not the dramatic shock of a ransomware-like network disruption, but in aggregate, such nation-state attacks are estimated to cost the US economy ~$600bn annually.[14]

13. FBI, China's Quest for Economic, Political Domination Threatens America's Security. 2022. Note: At the time, Mr. Wray stated this as "one new investigation every 10 hours". Sources today indicate it is more like one every 8 hours.
14. US IP Commission 2019 Review: Progress and Updated Recommendations, February 2019.

Reality 2: Nation-state attacks are not indefensible. They start by exploiting common weak spots: attackers often gain entry via people inside the targeted organization.

Nation-state attackers are skilled after they gain access inside a corporate network. However, the method by which they sometimes access the entrance can be simple: an individual wittingly or unwittingly let them in.

Insiders are not always the source of entry for nation-state attacks, however they do provide another important vector when the cyber vector is infeasible, or when other objectives are required. This includes when the sought after IP is not in the digital domain or is air-gapped. As every attack must start with a way in, corporate risk management programs that emphasize financial and human resources on insider detection, protection, and prevention can improve a company's chance to protect against state-actor attacks and cascading impacts.

With a risk management program designed to analyze the threat from a state-actor behavior POV, resources focused on measuring KPIs for detection and predicting risky insiders can be allocated accordingly. This type of approach is already used in other areas of corporations, like using technology and assessment methods to better predict workplace safety incidents before they cascade into much larger losses and liability costs. Applying a similar approach for digital age risks can return a high yielding risk ROI.

A recent example we increasingly encountered related to 'where and how to allocate risk resources' was in the aftermath of the start of the war in Ukraine. In the months after the conflict started, companies were often asking "is my risk of being collateral damage heightened?"; and "are we at greater risk of that truly catastrophic incident we've long feared?".

State actor attacks are not necessarily sophisticated attacks—80% of attacks are not believed to involve sophisticated weapons.[15] This means early detection of a threat is often more possible and key to avoiding or limiting damage. The same is true for criminal cyber actors like organized crime groups or hacktivists.

Companies rightly did not understand how much damage a targeted, sophisticated attack might cause them (it is near impossible to know or measure this). However, in our conversations, they also rarely acknowledged how vulnerable they truly are to these more subtle "insider entry" nation-state attacks, or even how attractive a target they may be. Again, even with the breakout of war involving Russia, a known hostile adversary that is highly skilled in cyber attacks, the actual, more frequent risk companies are facing is not the highly improbable 'Cyber Armageddon' scenario.

15. Dr. Michael McGuire, Nation States, Cyber Conflict and the Web of Profit (HP and HP Wolf Security). 2021.

Rather it is the 'here and now' risk of smaller, insider targeted attacks that open the company network up to IP theft, espionage and future damage that is much more likely. It is understandable that companies continue to be worried about potential cyber war collateral damage from that conflict, but a robust risk management solution could be budgeted on what detection and predictive tools can be applied to the more likely threats of insider entry instead of time spent planning for the highly unlikely, undefendable Cyber Armageddon.

Many companies today are vulnerable simply because they are not difficult to target—at scale—through cyber, insider risk (a witting accomplice or an unwitting victim), as well as third parties (supply chain) using asymmetric techniques. SolarWinds clearly illustrates that with a little bit of effort on the attacker's part, they can reap huge returns on the collection of information and access to corporate systems simply because the owners and operators of those systems inherently trusted but did not verify the actions of employees (insiders) of their third-party vendors such as SolarWinds.[16] Furthermore, SolarWinds was a software supply chain attack that was coupled either with a cyber attack or an insider, such that software was modified before it was authenticated by SolarWinds.

Nation-state entities can successfully be rebuffed and/or slowed with effective cyber counter-intelligence-based detection approaches. However, they can appear to be a more powerful threat than they are because of how they often rely on corporate victims' soft insider targets to gain entry into an organization's network.

Nation-state actors use unsophisticated tools to gain network access, like USB drives, pared with witting and unwitting company employees, and once in, deploy more sophisticated tools and tradecraft to elude detection over long periods of time.

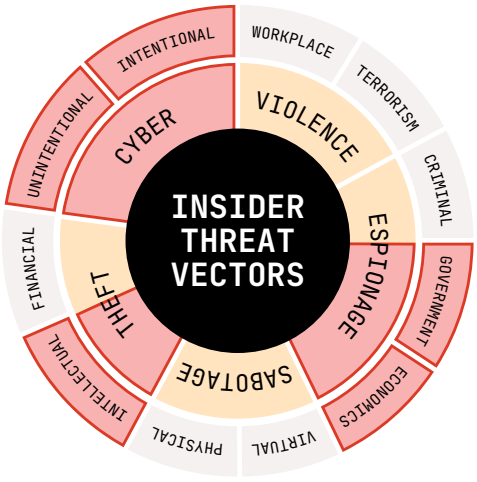


Figure 4. Insider Threat Vectors. Credit: CISA

As highlighted in Figure 4, this is an example of why in the Asymmetric Era, the human domain—the insider risk, as part of the enterprise supply chain—cannot be ignored in a corporate risk management program. The exploitations involving companies via this vector most often involve 'Cyber', 'Theft' and 'Espionage' for varied purposes.

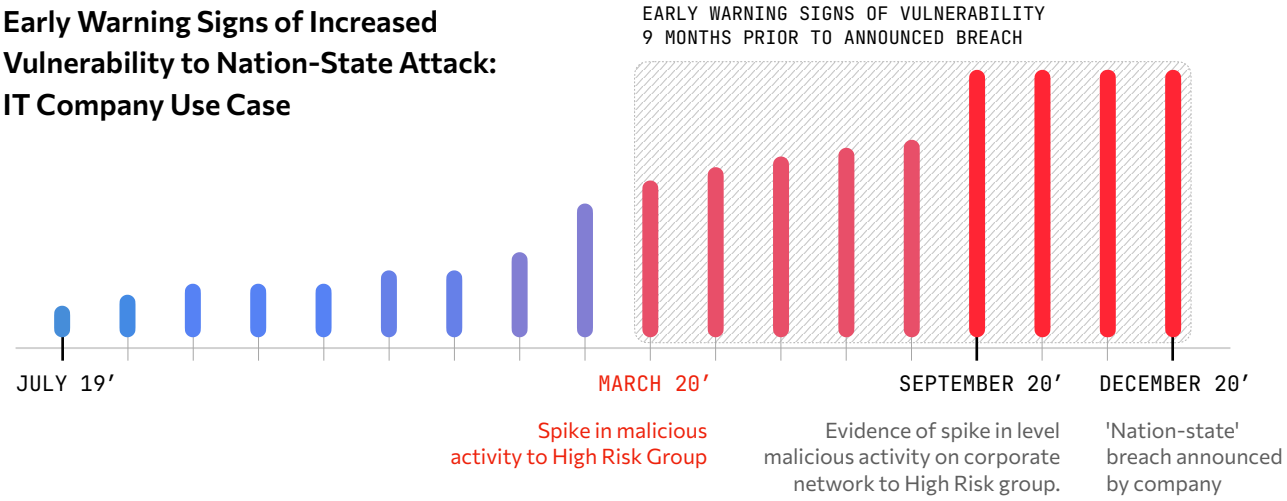
The solution begins by a) recognizing the threat to the company and asking the appropriate questions to ascertain and rank that threat; b) creating a detection-based system—ideally a predictive one based on counter-intelligence methods, not just a protective one; and c) continuously monitoring and mitigating the threat. All this should be done in line with the risk tolerance levels agreed to by the management team.

16. Clancy, C, Ledgett, R.H., Nissen, C., Sledjeski, C., Beyond SolarWinds: Principles for Securing Software Supply Chains, (MITRE), 2021.

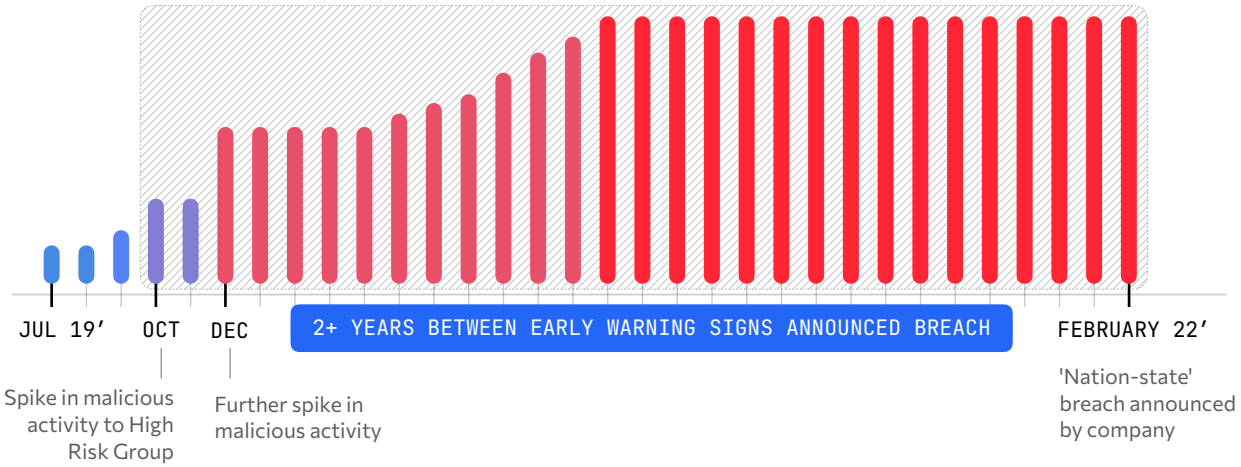
Early Warning Signs of Increased Vulnerability to Nation-State Attack

Another example of how effective detection can be used to identify potential vulnerabilities to state actor attack is seen through a recent use case. Based on proprietary Intangic data, recent larger nation-state attacks on companies have shown how tracking patterns that mimic typical state-actor attack behavior across a large number of both criminal and corporate networks can predict the attacker gaining successful entry to a targeted network in advance of a large, publicly-disclosed operational disruption. This can be seen in multiple cases, where observing large-scale behavioral patterns provided advance warning of damaging events several months - and in some cases years—prior.[17]

Early Warning Signs of Increased Vulnerability to Nation-State Attack: IT Company Use Case



Early Warning Signs of Increased Vulnerability to Nation-State Attack: Communications Company Use Case



17. Intangic's leading data science allows it to observe these spikes in malicious activity on corporate networks from an external view only – observing a more complete universe of malicious activity across 7,000 companies every day.

There are any number of motivations for a nation-state to attack or infiltrate an enterprise, ranging from purely financial, to IP theft and compromising their systems, using them as a conduit to other targets, driving them to bankruptcy, as well as an unintended attack as discussed above as 'cascading impacts'.

Failing to detect threats and vulnerabilities early can have financial consequences.

Typically, nation-state-oriented fear emanating from C-suites is associated with the widely-publicized, large catastrophic-like events like NotPetya. This attack affected a large number of well-known companies and produced vivid images of operations grinding to a halt at Maersk, and employees racing to disconnect computers from rapidly-advancing malware.

However, a more instructive example is SolarWinds, where surveillance and data gathering was carried out stealthily. This may result in a lower severity of impact over a longer period of time. Or in the case of SolarWinds, in a large loss event, but long after the initial breach. In addition to the disclosed $49 million in expenses from the cyber event, the company's C-suite and Board faced a major D&O lawsuit. SolarWinds CISO was named in a shareholder class action suit, alleging violations of the Securities Act. The shareholder litigation was settled for $26 million, payable under the company's D&O policy.[18]

Preparing for tomorrow's criminal cyber threats

The challenges presented by nation-state actors' asymmetric actions will not only continue to grow, but as the tools and capabilities become more sophisticated, they will enable similar growth in the cyber-criminal world. Cyber capabilities have been commoditized. The tools, tactics and capabilities used by state actors today will be used by criminal actors tomorrow. A more informed understanding of attacker behavior and being better prepared for nation-state strategies, tactics and approaches today, can make a company more resilient in the face of criminal cyber threats tomorrow.

Today's nation-state tactics are tomorrow's criminal tactics

A look at nation-state tactics and company vulnerabilities provides a look at the future.

Tools, tactics and strategies used by state actors today are used by criminal actors tomorrow.

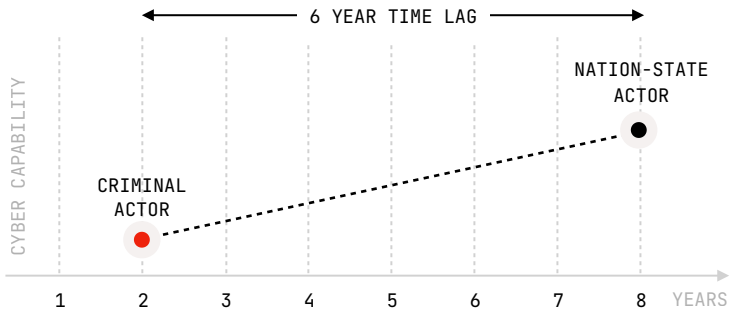


Figure 5. Criminal vs. Nation-State

18. SolarWinds Corporation, SEC Form 8-K October 28, 2022.

Sophisticated nation-state actors like China and Russia are widely categorized as 'established actors'—well-resourced, with deep pools of talent, and the most advanced, accurate and agile tools.[19] They have the time and money to sustain targeting and attacks on a range of commercial and government targets over a longer period of time across the world.[20] This includes tactics like cultivating insiders within companies to obtain valuable IP and/or plan larger attacks in the future.

Another category of nation-states includes those with their own agendas, tactics, tools, timelines, etc.—albeit at a significantly smaller scale than China and Russia. These include Iran and North Korea, and nation-state affiliates such as Conti and KillNet.

The third category is the emergent actor, including certain criminal organizations—less well-resourced, with limited tradecraft, though still capable of posing a significant threat to organizations as the rapid growth of ransomware has proven. According to the US Department of Homeland Security, though these actors are less technologically-capable, they look to state actors like China and Russia for ideas, capabilities, and resources.[21]

This dynamic between nation-state and criminal actors further underlines the importance of gaining a better understanding of the former, not just for today's state actor attacks, but also in preparation for tomorrow's criminal threats.

Reality 3: Thinking differently about the nation-state risk helps remove the perception blind spot and opens better risk transfer options

Companies are increasingly accepting that nation-state risk is an uninsurable risk 'you simply have to live with', and that you do what you can to mitigate it and hope it doesn't materialize. This is an understandable position when the insurance market has made it increasingly difficult to obtain coverage. But thinking differently about the risk can make 'the unmanageable' more manageable.

As the value of technology assets has grown exponentially, companies are increasingly seeking to lower uncovered risk exposure that by some recent estimates is over $1 trillion USD.[22] Many carriers are increasingly hesitant to underwrite (and markets unwilling to permit [23]) a risk that is not well understood or has the potential for cascading impact. This is evidenced in part by growing policy exclusions specific to the risk.[24]

19. US Department of Homeland Security, Public-Private Analytic Program Topic Team Overviews. 2022.
20. Ibid.
21. ibid.
22. Global Federation of Insurance Associations, Global protection gaps and recommendations for bridging them, March 2023.
23. James Rundle, Lloyd's to Exclude Catastrophic Nation-Backed Cyberattacks From Insurance Coverage (Wall Street Journal). August 18, 2022
24. Helen Thomas, The corporate world is losing its grip on cyber risk (Financial Times), February 1, 2023. (https://www.ft.com/content/78bfdf29-1e20-4c12-a348-06e98d5ae906)

Despite the growing threat and rising demand for cyber insurance, coverage remains low across all forms of cyber risks, not just nation-state. The Organisation for Economic Co-operation and Development (OECD) estimates that the share of global cyber losses that are uninsured may be as high as 85-90% of all cyber losses incurred.[25] Many estimates put the global cyber protection gap at 98-99%.[26]

In one sector alone, Lloyd's estimated that a significant attack on 15 ports across the Asia-Pacific could result in $110bn in losses, 92% of which would be uncovered or $101bn in uninsured costs.[27]

Evolving legal and regulatory frameworks and the case of Merck needing five years in the courts to secure payment on a claim from NotPetya highlight some of the challenges with current insurance.[28] This has led an increasing number of companies to conclude that the risk is uninsurable. The end result is an increasing amount of loss exposure sitting on corporate balance sheets.

Thinking Differently and Reallocating Resources can produce greater resilience

But thinking differently about the risk – informed by a better understanding of the nation-state adversaries' behavior - creates opportunities for a stronger risk management program and greater corporate resilience. An active approach to building greater resilience is possible in the face of today's nation-state attacks and tomorrow's criminal adversaries:

1. **Up-to-date data on the threat activity around your company - in recognition that the risk is dynamic and constant, and that a 'moment-in-time' assessment is not sufficient.** *Takeaway:* If you are already at elevated risk of a nation-state breach relative to peer companies, it is now possible to know that and take preventative measures to lower the likelihood of material breach, including more investment in threat detection. Intangic and Souhegan Group have deep expertise in these areas and assist customers with both insurance and risk management services.
2. **Early detection of an attack—in recognition that nation-state attacks can be defended against with the right approach.** *Takeaway:* Small problems, that can be detected, can lead to large problems and cascading risk if not remedied. This is true, be they the result of nation-state or criminal actors. In cyber, investing in often-overlooked detection is as important as protection, and is essential for better management of nation-state threats. Equally essential is informed understanding and assessment of 3rd party risk coupled with early detection which will protect against the other major attack vectors we have raised in this paper.

25. OECD, Enhancing Financial Protection Against Catastrophe Risks: The Role of Catastrophe Risk Insurance Programmes, 2021.
26. John Neal, Cyber: building resilience for an unrealised threat. November 10, 2022.
27. Lloyd's of London. Shen Attack: Cyber risk in Asia Pacific ports, October 14, 2019.
28. Andrea Vittorio, Merck's $1.4 Billion Insurance Win Splits Cyber From 'Act of War' (Bloomberg Law), January 2022.

3. **Enabling a timely recovery - getting the business running efficiently again quickly after a material breach occurs, lowering the likelihood of a cascading risk event.** *Takeaway:* With a risk management and transfer tool that detects problems early and provides a fast payout, an injection of cash when it is needed, helps teams correct problems and limit economic damage from a material breach so companies can recover from small events and **lower the likelihood of much costlier events in the future.**

About the Authors

Christopher Nissen,
CEO and Founder, Souhegan Group Risk Solutions.

Christopher is founder and CEO of Souhegan Group LLC, a company dedicated to discovering and mitigating risks from nation-states against companies. He has over three decades of experience developing solutions for extremely complex national security challenges from a counterintelligence vantage point at the MITRE Corporation where he was Director of Asymmetric Threat Response & Supply Chain Security – a position he created. At MITRE, he worked across the corporation developing essential strategic elements to address non-kinetic, full-spectrum asymmetric threats to national security both in the public and private sectors.

He is currently a Professor of Practice at the Applied Research Center for Intelligence & Security (ARLIS) at the University of Maryland. Chris has provided strategic consultation to executive management teams of several large commercial companies and spoken extensively on asymmetric risk via nation-states and mitigation solutions. He holds BSEE and MSEE degrees and has a background in structured analytical techniques.

Chris is the lead author of the report "Deliver Uncompromised, A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War"[29], a primary catalyst for the national attention now being paid to asymmetric actions including supply chain security and their associated operational risks.

Contact: can@souhegangroup.com

29. Deliver Uncompromised, A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War. https://www.mitre.org/news-insights/publication/deliver-uncompromised-strategy-supply-chain-security-and-resilience.

Chris Nolan,
Vice President of Marketing, Intangic

Chris oversees global marketing at Intangic, including thought leadership, the development of public-facing products, and issue-based engagements with corporate customers. He co-authored an article in a leading peer-reviewed journal on the intersection of cyber and finance titled Cybersecurity: today's most pressing governance issue. He leads the company's engagement on strategic public policy issues. Chris also co-authored The Economic Costs of Cyber Risk with the Foundation for the Defense of Democracies (FDD). He has spoken at investor conferences on the financial and economic risks associated with cybersecurity.

Chris' work has appeared in The Washington Post, Lawfare Blog, The Hill, and the insurance trade press.

Ryan Dodd,
Founder and CEO, Intangic

Ryan leads data science, technology and product vision for Intangic. He is a entrepreneur with extensive real-world cyber and financial modeling experience. Prior to founding Intangic, Ryan had 20 years as a hedge fund manager, including with Man GLG and structuring financial risk products. He created the CyFi™ model at the core of Intangic and Intangic MGA.

Ryan co-authored the first peer-reviewed article on the intersection of cybersecurity and finance in a leading journal. (*Cybersecurity: today's most pressing governance issue*)
His work has appeared widely in the insurance and financial press including the Financial Times, Washington Post, The Insurer and The Insurance Journal.

What does Intangic have to do with Nation-state risk?

Intangic's technology and proprietary model are at the core of Intangic MGA. Intangic MGA recently launched a new insurance product, CyFi™, that does provide companies with incentives for both better detection and protection. It offers a policy, currently available to publicly-listed companies in the United Kingdom and United States, that does not exclude cyber war or nation-state cyber attacks.[30]

At the center of this is an innovative way to assess cyber risk and predict technology-related losses, first by recognizing that attacks are constantly occurring, whether they are carried out by nation-states or criminal actors. And because attacks are constant, what matters is not 'if' attacks occur, but rather when these attacks start to materially impact a company's operational performance.

This is a solution that deals with nation-state threats as they are right now, not the catastrophe-like events that have already occurred and which are highly unlikely to occur as a result of successful deterrence and retribution efforts by Western governments.

By thinking differently about the risk, it is possible to offer a risk transfer product that places an emphasis on both early detection and remedy of problems to lower the chance of a cascading event stemming from damage caused by a nation-state attack, intentionally or unintentionally.

For more information, please visit: intangicmga.com

Contact: cnolan@intangic.com

About Souhegan Group Risk Solutions

While there are several companies that claim to "illuminate" supply chains, score cyber risks etc., the company stands apart because of its deep understanding of the counterintelligence tradecraft in use today by bad actors—whether they're nation-state or not.

Security baselines start at the company's degree of risk as a target itself in a larger geopolitical context and your vertical industry ecosystem, then progresses through a number of blended-operation threat vectors of which formal supply chains are one.

The company uses this background to design an early detection capability for each of these attack vectors tailored for your enterprise and management's risk appetite.

30. CyFi™ Policy is to be launched this year in the US.