Cyber Protectionism: Global Policies are Adversely Impacting Cybersecurity

Erik Avery

Cyber Protectionism: Global Policies are Adversely Impacting Cybersecurity

GIAC (GSTRT) Gold Certification

Author: Erik Avery, erik.avery@student.sans.edu
Advisor: *David Hoelzer*

Accepted: *29 July 2019*

Abstract

Cyber Protectionist policies are adversely impacting global cybersecurity despite their intent to mitigate threats to national security. These policies threaten the information security community by generating effects which increase the risk to the networks they are intended to protect. International product bans, data-flow restrictions, and increased internet-enabled crime are notable results of protectionist policies – all of which may be countered through identifying protectionist climates and subsequent threat. Analyzed historical evidence facilitates a metrics-based comparison between protectionist climate and cybersecurity threats to comprise the Cyber Protectionist Risk Matrix - a risk framework that establishes a new cybersecurity industry standard.

1. Introduction

Cyber protectionism in global politics is adversely impacting cybersecurity despite maintaining a public intent to mitigate threats to national security. Cyber protectionism is the use of national cyber policies to protect domestic organizations from foreign economic and cyber-enabled threats. Political differences between major powers, including the United States, Russia, China, the European Union, and the United Nations, have contributed to major cyber protectionist movements and declining cybersecurity over the last ten years. These movements have taken shape in policies which ban the use of foreign products, restrict the flow of cross-border data transfers, and reject high-profile business transactions. Although news organizations and academic institutions address the impact of these events on a national and bilateral scale, none compare the larger interconnectivity of policies and their cybersecurity impacts both qualitatively and quantitatively. This paper addresses the effect that cyber protectionist policies have had on cybersecurity over the last ten years rather than their justification. As analysis on present trends is conducted and additional security data is published, the model which this paper uses can be extended to compare cybersecurity trends against cyber protectionism into the future.

While governments and international organizations control legality and policy from one end of the hierarchy, this paper seeks to demonstrate a solution for the cybersecurity practitioner and provide a mechanism with which private organizations can combat a range of protectionist climates. The Cyber Protectionist Risk Matrix (CPRM) is the proposed solution based on the trends analyzed in this paper, which provides security professionals with a standard, repeatable, and flexible model for predicting the risk of being targeted by cyber-attacks that are encouraged by cyber protectionism. By utilizing this matrix, any organization can present a clear and quantifiable threat picture to organizational leaders, helping to shape business decisions and enterprise security funding.

Erik Avery, erik.avery@student.sans.edu

2. Cyber Protectionism

Cyber protectionist policies distinguished themselves from other movements as early as 2009, when they predominately rose due to competition in the U.S.-China technology industry. However, the origin of cyber protectionist policy can be traced back decades earlier to the creation of the Committee on Foreign Investment in the United States (CFIUS) in 1975 (Executive Order 11858, 1975). This committee was not inherently focused on enforcing protectionist policies through cyber-exclusion in its infancy but became the mechanism through which the U.S. government did so in 2008. The alleged national security investigation by CFIUS into Huawei's - a major Chinese Internet Communications Technology (ICT) company - bid to acquire the U.S. company 3Com ostensibly led to the abandonment of the deal altogether (Weisman, 2008). By establishing this precedent in contributing to the abandonment of a business acquisition, allegedly due to national security threats, the U.S. Government made it legally tolerable to prohibit business on the grounds of cyber protectionism. Since CFIUS did not publish a report on the deal, and with no Presidential decision on the acquisition, it is not clear what was uncovered by the organization. However, a significant number of protectionist moves in the name of cybersecurity left their mark on the following decade.

According to the Congressional Research Service, Presidential action only blocked six acquisitions in the organizations' 43-year history, five of which occurred since 2012 (Jackson, 2019, p. 18). Remarkably, all five were blocks against business acquisitions involving Chinese firms (see Figure 1). The drastic actions by the U.S. have continued with the banning of Chinese telecommunications company, ZTE, in 2018 and the total ban on Huawei by U.S. President Donald Trump in 2019 (Stecklow, Freifeld, & Jiang, 2018; Executive Order 13873, 2019). While the companies were not all ICT entities, the severity and increase in presidential directive-blocked transactions show a degradation in the climate manifested by shortening the reach of Chinese technology into U.S. networks. Perhaps that by shortening that reach, in the name of security, it also encouraged the growth of small-scale protectionist policy exchanges between private and public entities.

Erik Avery, erik.avery@student.sans.edu

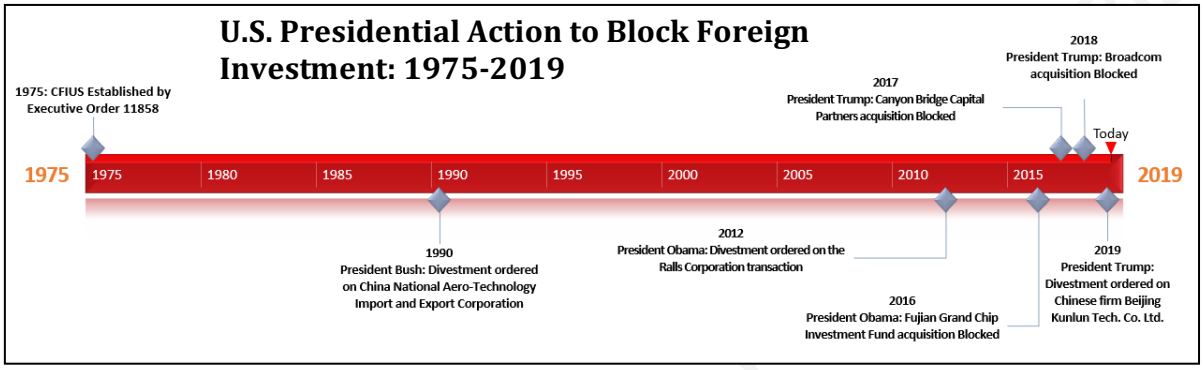

Figure 1: U.S. Presidential actions to block foreign investment in the United States since the conception of CFIUS in 1975 (Jackson, 2019, p. 18)

Actions by China's government occurring years before U.S. action predicated the harsh denials by the U.S. executive branch. In 2006, China adopted the indigenous innovation policy which intended to boost China's competitive stance in the global economy by increasing innovation by Chinese companies, domestic ownership of intellectual property rights, and overall technological advancement (Bichler & Schmidkonz, 2012, p. 2). This policy became burdensome for foreign companies years later as it became a means for the Chinese government and companies to assume rights to intellectual property from companies seeking to tap into the Chinese market, according to a report from the U.S. Chamber of Commerce (McGregor, 2010). With the promise of revocation of this law by Hu Jintao to U.S. President Barrack Obama in 2011, this type of policy originally appeared to be abandoned (Palmer D., 2011). However, this Chinese cyber protectionist ideology resurged in 2017, with the new iterations of China's National Security and Cybersecurity policies (Chin, Liu, & Zhang, 2018). As this research will suggest in later sections, these recurring instances of market barriers have contributed to malicious cyber activity by encouraging intellectual property theft in isolated technology markets.

The U.S.-China cyber protectionist movement was not the only protectionist war waged during this decade. In 2017, the U.S. President signed a law into effect which banned the use of Kaspersky Labs products, a Russian anti-virus company, from being used on the networks of U.S. civilian government agencies across the board (Department of Homeland Security, 2017). Russia's well-publicized and long-standing System of Operative-Investigative Measures (SORM) was probably also a contributing factor of this action, and was intended to curb the threat of associations between the Russian

government and the software company, according to the public statement (Soldatov & Borogan, 2013). Whether or not the warnings of the U.S. Department of Homeland Security are well-founded, the implications place a heavy burden on cybersecurity professionals facing equipment acquisition decisions, particularly with the removal of products from the shelves of several major U.S. companies (Volz, 2017; St. John, 2017). The Russian company appeared to shrug off the impact of the ban in a statement made in 2019, in which they claimed a fall of 25% in sales only in North America, while the rest of the global market continued to show growth (Kaspersky Lab, 2019). However, the company continued to press forward with its transparency initiative to boost trust in its remaining global markets (Kaspersky Lab, 2017). In contrast with other global policies, this was a sign of a reduction in the cyber protectionist climate severity between these two global powers, based on the lack of retaliatory political action.

The United States was not alone in implementing harsh cyber protectionist policies in the face of supply chain threats. Both China and Russia implemented national policies which have increased resistance to foreign companies attempting to do business with these nations. The Chinese Indigenous Innovation Product Accreditation Act of 2009 and the National Security and Cyber Security Laws of 2017 contain provisions to protect the Chinese economy and cybersecurity. On Russia's side, the previously-mentioned SORM policies, along with data housing rights, have contributed to American and other countries' companies not entering its market due to burdens induced by legal compliance. The Russian government also more prominently focused on internet governance and data rights, rather than out-right banning of foreign companies. Policies such as the 2012 establishment of an internet blacklist, the 2017 outlaw of VPN services, and the 2019 pursuit of a Russian intra-net all point to a severe cyber protectionist stance that seeks to defend itself from the risk of open internet (BBC, 2012; BBC, 2017; Kiselyova, 2019).

Finally, analysis of international organizations' cyber protectionist policies indicates an overall emphasis on the desire for global privacy and standardization of internet security practices. The most prevalent protectionist policy, stemming from a desire to protect the data privacy of its citizens, is the European Union's General Data Protection Regulation (GDPR), enacted in May 2018. According to the GDPR public

website, the new data privacy law was designed to: harmonize data privacy laws across Europe, protect and empower all EU citizens data privacy, and reshape the way organizations across the region approach data privacy (EU GDPR.org, 2018). While the regulation still does not specify technical requirements for keeping data secure, it hindered the ability of security professionals to use one of their most critical tools – Whois. The strict implementation of privacy regulations has had a direct impact on the ability of the Internet Corporation for Assigned Names and Numbers (ICANN) to ensure the availability of the entire Whois system. According to the Chair of the ICANN Board of Directors, the Whois system is a critical tool in the fight against "cybercrime, malicious actors, intellectual property infringement, and more" (Chalaby, 2018).

To date, another substantial international organization has failed to write meaningful cybersecurity policies, despite their potential for having an impact on the global cybersecurity industry. The United Nations passed Resolution 68/167 in 2014, calling on its members to respect privacy as a basic human right in the digital world, but offered no strict implementation guidance (United Nations, 2014). Since then, the United Nations member states have debated, presented their resolutions, and discussed the issue at global summits. At the 2018 Internet Governance Forum, UN Secretary-General Guterres recommended that an inclusive approach was needed from world powers to develop effective legislation, calling for a multidisciplinary approach using a common language to bring people into the discussion (Internet Governance Forum, 2019). Currently, the UN General Assembly's First Committee has adopted two draft resolutions from Russia and the U.S., respectively, which will go before the General Assembly in September 2019. The draft sponsored by the U.S. purposes to study the impact of international ICT laws based on previously established norms. Conversely, the Russian sponsored draft seeks to make "the [UN] negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent" (United Nations, 2018). Depending on which way the General Assembly leans in September could mean new resolutions passed in the name of cyber protectionism on the horizon. New regulations in the name of privacy are likely, which signals the passing of new legislation with only the appearance of bolstering cybersecurity.

Erik Avery, erik.avery@student.sans.edu

3. Identification of Protectionist Climates

Since the labeling of protectionist ideologies is binary – either it is protectionist, or it is not - expansion of identification into cyber protectionist climates is dependent on the clear delineation of several factors to determine a specific policy's relevance and severity. This paper uses the following criteria to determine overall policy severity on a linear, time-based model: 1) data privacy, 2) internet governance, and 3) market permeability to foreign businesses. These criteria have demonstrated to be front-runners in the past decade as active areas of contention for ICT legislation and cyber protectionist policies. Based on the evidence addressed in the previous section of this paper, and additional global policy analysis, this paper presents an identification model which assigns a severity rating to a protectionist climate based on the adoption or proposal of such policies. With each major category, three subcategories consisting of smaller-scale subjects which identified themselves as having a significant impact on the global protectionist climate will be identified. These subcategories are available in Appendix A – Climate Identification Subcategories. Based on the number of these policies present in each year of analysis, the global climate is assigned a rank one through five, beginning with minimal or globalist (zero to one policy observed) and advancing to aggressively protectionist (more than eight policies observed). The chart in Figure 2 depicts the research and identification of these climates globally, from 2009 to 2018.

As depicted by this model, the overall protectionist climate became more severe from 2009 to 2017. 2017 was the first year within the period of study classified as severely protectionist. This paper attributes this trend to the growing conflict between ideologies identified between major world powers, and to each power seeking to strengthen its position in upcoming negotiations and debates. 2018 does not appear to follow the overall established trend in the previous years. Perhaps a shortfall in this paper's research is to blame for this categorization, as researcher bias in time and attention limits discovery of new policies and understanding of global legislative systems.

Erik Avery, erik.avery@student.sans.edu

Currently, this model does not address scope, duration, target, or enforceability within each year. This paper recommends precise studies are conducted subjecting an expanded list of countries to analysis, from which to yield a more accurate protectionist climate map as set forth by this model.

Global Cyber Protectionist Climate Identification: 2009-2018

Rating	2	1	2	2	2	1	2	3	4	2
Count	X X		X X	X X	X X X	X X	X X	X X X	X X X X	X X
Category	Privacy Rights Internet Availability Market Resistence	Privacy Rights Internet Availability Market Resistence	Privacy Rights Internet Availability Market Resistence	Privacy Rights Internet Availability Market Resistence	Privacy Rights Internet Availability Market Resistence	Privacy Rights Internet Availability Market Resistence	Privacy Rights Internet Availability Market Resistence	Privacy Rights Internet Availability Market Resistence	Privacy Rights Internet Availability Market Resistence	Privacy Rights Internet Availability Market Resistence
Year	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018

Figure 2. This table depicts how the cyber protectionist climate is identified through the comparison of which types of policies became active and when. For a more detailed model, please refer to Appendix A.

With such actions taken by global governments attempting to ensure cybersecurity across borders, one would expect the overall state of cybersecurity to be in a more stable condition than that of ten years ago. On the contrary and despite these policies, the overall state of security has been in rapid decline along with identified protectionist climates.

4. The State of Security

In accordance with the general increase in aggressive protectionist climates, observable trends in global cybersecurity show a negative slope in security since 2009. These trends indicate cybersecurity worsening in conjunction with the emergence of harsh protectionist climates, rather than eased tensions. This section of the paper presents a synopsis of the state of security, relying on global law enforcement reporting, theories of security, and an advancement of nation-state associated cyber operations.

Overall reporting trends indicate an increase in frequency in internet-based intrusions – particularly in internet crime since 2009. Voluntary internet crime reporting

Erik Avery, erik.avery@student.sans.edu

to the U.S. Department of Justice Internet Crime Complain Center (IC3) increased in both quantity and monetary loss over the last ten years. In 2009, the IC3 received roughly 336,000 complaints globally, ranging from instances of fraud to computer damage (Internet Crime Complaint Center, 2010, p. 4). In 2018, the total number of complaints received rose to over 350,000 - an overall increase of 4.5 percent, with an emphasis on business and personal email account compromises (Internet Crime Complaint Center, 2019, p. 5). It is important to note that the IC3 characterization of cybercrime does not warrant direct comparison of cyber-criminal activity as reported by other cybersecurity firms which may have more in-depth analysis and incident response data.

Since the victims and IC3 probably do not have complete knowledge of the incident at the time of reporting, it is evident that other categories of cyber threats (i.e., Advanced Persistent Threats (APTs) and Hacktivist activity) exist within these metrics. A general trend in evolving tactics and technology in the cybercriminal community explains the increase in reporting per crime category. For example, the continued development, improvement, and success of tools and techniques over time contributed to the rise in ransomware statistics (Lee, 2018). While the annual reports contain consistent frequency-based ratings emphasizing certain crimes over others, non-uniform reporting and categorization challenge precise comparison across the decade.

More alarming is that the increase in reporting volume was eclipsed by the total monetary impact of the crimes. The total financial impact to the victims increased by 384.2 percent over the same ten-year reporting period. According to IC3, from 2009 to 2018 the total monetary loss reported by the victims in cases which it referred to law enforcement increased from $559.7 million to $2.71 billion (Internet Crime Complaint Center, 2010, p. 4; Internet Crime Complaint Center, 2019, p. 5). Figure 3 below depicts the progression of reporting statistics in terms of volume and monetary loss.

Undoubtedly, IC3's improved methodology over time and criminal tactic evolution both lend themselves to increased reporting activity. However, the sharp rise in monetary impact to victims suggests improved effectiveness and prevalence in internet-based activity aimed at financial gain. As internet-based technology changes, it enables criminals – as defined by the reporting - to conduct money-making operations for less cost and with less skill than in 2009.

Erik Avery, erik.avery@student.sans.edu

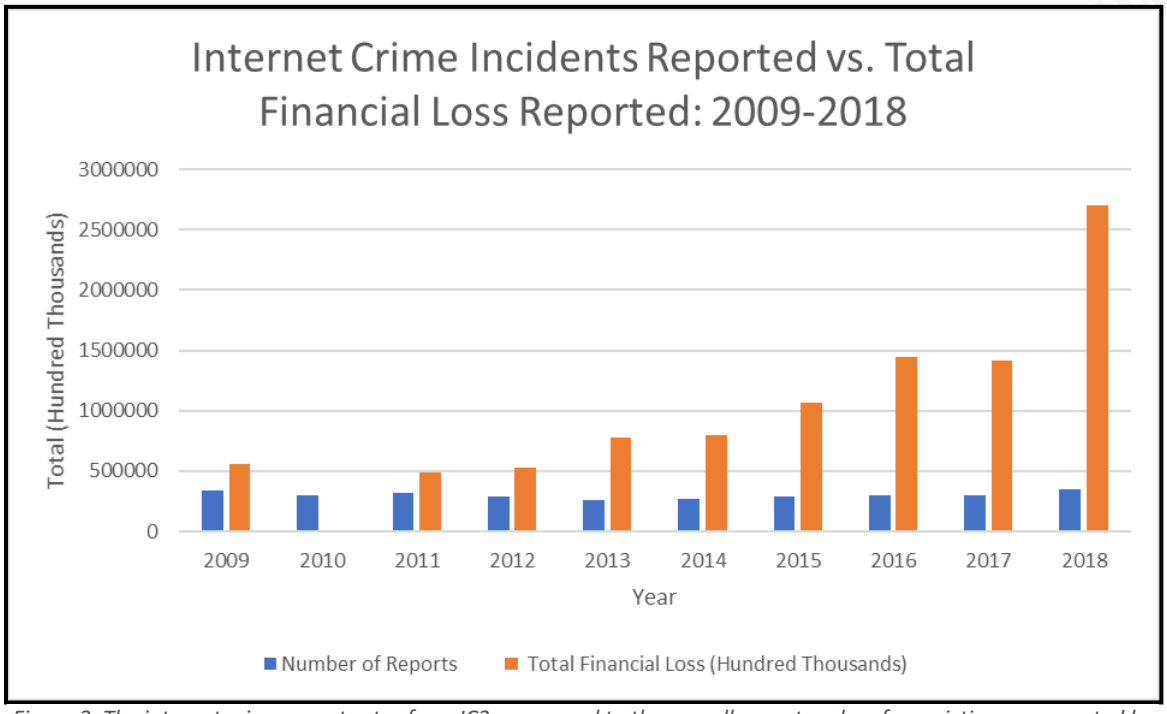

Figure 3. The internet crime report rates from IC3, compared to the overall monetary loss from victims, as reported by victims (2009-2018). The increase in financial loss is disproportional to the increase in reporting over the last ten years. Total financial loss data not available for 2010 (IC3, 2010; IC3, 2011; IC3, 2012; IC3, 2013; IC3, 2014; IC3, 2015; IC3, 2016; IC3, 2017; IC3, 2018; IC3, 2019).

The crime reporting rate suggests that cybersecurity in its current state is not able to cope with the advancement in global criminal operations and severe protectionist climates. It is important to note that while increased reports are probably reflective of an increase in events, IC3 estimates that only 15% of internet crime is being reported (Internet Crime Complaint Center, 2014, p. 6). This could be due to victims being unaware of the available avenues for internet crime reporting, not wanting to become involved in a law enforcement investigation, or not knowing that the criminal activity occurred. The actual crime rate, what is known as the dark figure, of internet-enabled criminal activity and the number of reportable crimes is probably much higher. IC3 reporting is also indicative of crime trends from other countries, in which there is no appropriate law enforcement agency for direct referral. Other countries include India, the United Kingdom, Canada, Australia, Georgia, and at least 15 others (Internet Crime Complaint Center, 2019, p. 17).

The growth of protectionist climates has also fueled APT development over the past decade. The United States' and European Union's adversaries in trade and politics

have shown to be aggressively improving, according to data from multiple private cybersecurity companies.

Over the past ten years, North Korean APT activity emphasized financially motivated operations as opposed to destructive and disruptive ones in 2009 (FireEye, 2019, p. 23). The increase in cybercrimes inflicting monetary loss on victims is also consistent with the growth of financially impactful crimes reported by U.S. law enforcement. While the portion of global financially motivated hacking on North Korea's part is unknown, as are specific protectionist climate policies they enacted, they are not likely isolated from global crime trends. This data suggests that protectionist climates may negatively impact global economies and may encourage financially motived cybercrime.

Russian APT activity has expanded from targeting NATO and eastern European targets to conducting operations against global targets of strategic interest, including those in the U.S. and Europe (FireEye, 2019, p. 26). Overall, protectionist policies involving the U.S. and Russia stem from what several U.S. Presidential Executive Orders have called "cyber-enabled activities," and may indicate a shift in targeting because of developing conflict in regions around the world (E.O. 13694, 2015; E.O. 13757, 2016).

Maintaining the most active and broad base of APT groups globally, Chinese threat actors have evolved from conducting loud intrusion attempts against foreign governments and stealing intellectual property, to "strategic espionage campaigns" carried out in Asia (FireEye, 2019, p. 29). In 2009, indications of operations being conducted based on Chinese and U.S. protectionist policies were already present. According to the investigating firm, that year, a U.S.- based company in negotiations with a Chinese corporation was targeted by an APT, assessed to be an effort to gain information about the opposite party's stance (FireEye, 2010, p. 22). It may be the case that perceived Chinese government interest in maintaining control over its industries contributed to the hacking of the U.S. company. Given a private security firm's assessment that they were primarily engaged in government-targets during this period, it may be an indication of the desire to shift to assist in the protection of their businesses, as suggested by Chinese law in 2009 (Ikenson, 2017, p. 3).

Erik Avery, erik.avery@student.sans.edu

A recurring theme according to the same firm, is that numerous intrusions against U.S. companies, law firms, and non-profit organizations occurred in part due to the relationships they had with other entities within China (FireEye, 2010, p. 23). Regardless of U.S.-industry affiliation, the targeting of these entities showcases the impact of Chinese policy on U.S. entity security.

Further confirmation of worsening cybersecurity exists in industry reporting present in both trend analysis and case studies. According to one firm's incident response data, companies who suffer one cybersecurity breach are frequently retargeted in another cyberattack soon after. In 2018, 64 percent of the firm's clients were re-targeted by a significant cyber-attack with 19 months, an overall increase of eight percent since 2017. This data also showed the financial industry as the most re-targeted industry and an increase of eight percent since 2017 (FireEye, 2019, p. 10).

Attackers' reconnaissance data from the initial intrusion or undetected persistent access may contribute to repeat victimization and shows that professional remediation of an attack does not always prevent future attacks from occurring. If the motivating policies of these attacks were financial or related to the market permeability and data privacy categories on the cyber protectionist climate model, it is probable that organizations impacted by that policy are highlighted for cyberattack for a variety of motivations. According to the Verizon 2009 Data Breach Incident Report, unauthorized access via default or shared credentials was the root cause of 53 percent of hacking incidents (Verizon, 2010, p. 17). The exploitation of these incidents does not suggest advanced adversary tactics, but instead points to a lack of cyber hygiene. An increased threat in a severe climate augments the risk to organizations which do not enforce basic security principles. This data also suggests that protectionist policies in the name of security are not effectively minimizing the problem's root cause. Improvement of security standards and internal policies or businesses globally would be more effective than mandating strict internet governance laws or denying companies' business in ICT markets.

To conclude, the negative trend in cybersecurity is evident in this data in correlation with our protectionist climates. The policies adopted in the name of security are not working to curb the threats to businesses and could be increasing the threat. While

the correlation of these two families of data does not necessarily equal causation, the fact remains that if the globalist policies are not improving cybersecurity, they are creating a more diverse and prevalent threat landscape for businesses caught in the middle of the hostility.

5. Cyber Protectionist Risk Matrix

To manage risk in a harsh cyber protectionist climate, organizations around the world need to have a model by which to analyze the risk to their organization based on relationships, security practices, and the climate in which they operate. While every organization may not be able to change climates, they should be equipped to identify them and present clear solutions to their stakeholders in an understandable way. Based on the observed security trends and identified protectionist policies, this paper presents a model for predicting the threat around organizations based on five identified categories. This paper intends for the Cyber Protectionist Risk Matrix (CPRM) to be used by organizations whose stakeholders require knowledge of risks associated with cyber protectionism, and what can be done to mitigate them. By analyzing the five principal criteria that this paper sets forth, information security professionals can assign quantitative levels of risk and present them to stakeholders, organization executives, and senior policymakers for informed decision making.

This framework centers the five categories of analysis on the data uncovered by the analysis of cyber protectionism and security trends over the last decade. Based on that data, organizations' protectionist climate, daily operations, security posture, and relationship with foreign entities play into the localized threat created by protectionist policies. The cyber protectionist climate does not necessarily mean that there is an imminent threat to an organization. Therefore, other factors will be analyzed to assess what risk the climate poses to identified systems. With that in mind, each criterion must be independently studied according to predefined standards to gauge the overall level of threat. Heightened risk in one category alone does not translate to high risk to an organization. Some factors mitigate the risks imposed by others. The identified factors are listed below, aligned with tier explanation of impact to security.

Criteria	Summary
1. Global Cyber Protectionist Climate	Identify the current global protectionist climate by using the predefined standards and criteria in this paper's model.
2. State of Security	Identify the organization's state of security. This criterion seeks to identify whether your organization's security policies are relevant, current, and enforced. Identify any relevant security incidents or ongoing investigations.
3. Foreign Organization Relationships	Identify the relationships that the organization has with foreign entities. Following identification of the depth of these relationships, complete analysis to identify the protectionist climate of their host nation.
4. Policy Impact on Industry	Identify the specific protectionist policies aimed at the organization or industry. Describe whether the policies' impact is because of the nationality or industry category; identify whether the protectionist policies impact this specific organization more than any other indigenous organizations.
5. Policy Impact on Customers	Identify the impact that protectionist policies have on the organization's customers and business partners. Identify any barriers that the customers face during interaction stemming from protectionist policies.

Each of the five criteria should be analyzed independently, to ensure proper identification of the risk. Once analyzed, the category is assigned a severity rating of one through five – five being the most severe – based on specific ratings located in the Cyber Protectionist Risk Matrix (Appendix B). The cumulative score and rating found on the Risk Discovery Worksheet (Appendix C) determines the total risk to the organization. The highlighted categories of risk assist security professionals by identifying the specific areas needing corrective action to support risk mitigation.

Erik Avery, erik.avery@student.sans.edu

6. Conclusion

The identification of cyber protectionist climates and analysis of risk to the organization is intended for entities managing ambiguous threats on a large scale. Seldom seen is the inclusion of cyber protectionist ideologies and other external political factors in threat prediction to information systems. The implementation of the presented risk model allows decision makers to see predictive threat modeling to their organization and adjust business practices as a result.

These cyber protectionist policies are adversely impacting global cybersecurity despite their intent to mitigate threats to national security. By noting and assessing the various policies by the United States, Russia, China, the European Union, and the United Nations, improvements can be made to reverse the declining security trends. Governments should use this model to adjust their policies to increase their effectiveness without forfeiting global power. Organizations should use this model to manage an ambiguous threat landscape and alter their security focuses according to their needs. If both governments and private industry can accurately assess the impact to themselves based on cyber protectionist climates, they will halt the last ten years of security degradation and can alter policies to improve global cooperation and security.

Erik Avery, erik.avery@student.sans.edu

References

Bichler, J., & Schmidkonz, C. (2012). *The Chinese Indigenous Innovation System and its Impact on Foreign Enterprises.* Munich Business School, University of Applied Sciences. Munchen: Munich Business School. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.738.6363&rep=rep1&type=pdf

British Broadcasting Corporation. (2012). *Russia internet blacklist law takes effect.* British Broadcasting Corporation. Retrieved from https://www.bbc.com/news/technology-20096274

British Broadcasting Corporation. (2017). *Putin bans VPNs in web browsing crackdown.* British Broadcasting Corporation. Retrieved from https://www.bbc.com/news/technology-40774315

Chalaby, C. (2018). *Chair's Blog: Approving the Temporary Specification for gTLD Registration Data and Next Steps.* Internet Corporation for Assigned Names and Numbers. Retrieved from https://www.icann.org/news/blog/chair-s-blog-approving-the-temporary-specification-for-gtld-registration-data-and-next-steps

Chin, M., Liu, C., & Zhang, X. (2018). *China's Cybersecurity Law.* Reed Smith. Retrieved from https://www.reedsmith.com/en/perspectives/2018/01/chinas-cybersecurity-law

Department of Homeland Security. (2017). *DHS Statement on the Issuance of Binding Operational Directive 17-01.* Washington: Department of Homeland Security. Retrieved from https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01

EU GDPR.org. (2018). *The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years.* Retrieved from https://eugdpr.org/

Erik Avery, erik.avery@student.sans.edu

Executive Order 11858. (1975, May 7). *Foreign investment in the United States*. Retrieved from https://www.archives.gov/federal-register/codification/executive-order/11858.html

Executive Order 13873. (2019, May 15). *Securing the Information and Communications Technology and Services Supply Chain*.

FireEye. (2019). *M-Trends 2010.* Milpitas: FireEye. Retrieved from https://content.fireeye.com/m-trends

FireEye. (2019). *M-Trends 2019.* Milpitas: FireEye. Retrieved from https://content.fireeye.com/m-trends

Ikenson, D. (2017). Cybersecurity or Protectionism? Defusing the Most Volatile Issue in the U.S.–China Relationship. *CATO Institute*(Policy Analysis No. 815). Retrieved from https://www.cato.org/publications/policy-analysis/cybersecurity-or-protectionism-defusing-most-volatile-issue-us-china

Internet Crime Complaint Center. (2010). *2009 Internet Crime Report.* Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2009_IC3Report.pdf

Internet Crime Complaint Center. (2011). *2010 Internet Crime Report.* Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2010_IC3Report.pdf

Internet Crime Complaint Center. (2012). *2011 Internet Crime Report.* Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2011_IC3Report.pdf

Internet Crime Complaint Center. (2013). *2012 Internet Crime Report.* Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2012_IC3Report.pdf

Internet Crime Complaint Center. (2014). *2013 Internet Crime Report.* Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2013_IC3Report.pdf

Internet Crime Complaint Center. (2015). *2014 Internet Crime Report.* Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2014_IC3Report.pdf

Erik Avery, erik.avery@student.sans.edu

Internet Crime Complaint Center. (2016). *2015 Internet Crime Report.* Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2015_IC3Report.pdf

Internet Crime Complaint Center. (2017). *2016 Internet Crime Report.* Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2016_IC3Report.pdf

Internet Crime Complaint Center. (2018). *2017 Internet Crime Report.* Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2017_IC3Report.pdf

Internet Crime Complaint Center. (2019). *2018 Internet Crime Report.* Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2018_IC3Report.pdf

Internet Governance Forum. (2019). *IGF 2018 Chair's Summary.* Paris: Internet Governance Forum. Retrieved from https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/6212/1417

Jackson, J. K. (2019). *The Committee on Foreign Investment in the United States (CFIUS).* Congressional Research Service. Retrieved from https://fas.org/sgp/crs/natsec/RL33388.pdf

Kaspersky Lab. (2017, October 23). *Trust first: Kaspersky Lab launches its Global Transparency Initiative; will provide source code – including updates – for third-party review; to open three Transparency Centers worldwide*. Retrieved from Kaspersky Lab: https://www.kaspersky.com/about/press-releases/2017_trust-first-kaspersky-lab-launches-its-global-transparency-initiative

Kaspersky Lab. (2019, February 19). *Kaspersky Lab announces 4% revenue growth to $726 million in 2018*. Retrieved from Kaspersky Lab: https://www.kaspersky.com/about/press-releases/2019_kaspersky-lab-announces-4-percent-revenue-growth-to-726-million-dollars-in-2018

Kislyova, M. (2019). *Russian lawmakers approve new Internet law.* Moscow: Reuters. Retrieved from https://www.reuters.com/article/us-russia-internet-bill/russian-lawmakers-approve-new-internet-law-idUSKCN1RS0OS

Erik Avery, erik.avery@student.sans.edu

Lee, B. (2018). *Ransomware: Unlocking the Lucrative Criminal Business Model.* Santa Clara: Palo Alto Networks. Retrieved from https://www.paloaltonetworks.com/resources/research/ransomware-report

McGregor, J. (2010). *China's Drive for 'Indigenous Innovation': A Web of Industrial Policies.* U.S. Chamber of Commerce. Retrieved from https://www.uschamber.com/report/china%E2%80%99s-drive-indigenous-innovation-web-industrial-policies

Palmer, A. (2017, April 28). China's Cybersecurity Policy: Security or Protectionism. *S. Rajaratnam School of International Studies Commentary*(No. 081). Retrieved from https://www.rsis.edu.sg/wp-content/uploads/2017/05/CO17081.pdf

Palmer, D. (2011, January 21). *Analysis: Hu addresses U.S. stress over China high-tech drive.* Washington: Reuters. Retrieved from Reuters: https://www.reuters.com/article/us-usa-china-innovation/analysis-hu-addresses-u-s-stress-over-china-high-tech-drive-idUSTRE70J7RL20110121

Soldatov, A., & Borogan, I. (2013, September 12). *Russia's Surveillance State*. Retrieved from World Policy Institute: https://worldpolicy.org/2013/09/12/russias-surveillance-state/

St. John, A. (2017, October 12). *What the Kaspersky Antivirus Hack Means for Consumers*. Retrieved from Consumer Reports: https://www.consumerreports.org/privacy/what-to-do-about-the-kaspersky-data-hack-/

Stecklow, S., Freifeld, K., & Jiang, S. (2018). *U.S. ban on sales to China's ZTE opens fresh front as tensions escalate.* London/New York/Hong Kong: Reuters. Retrieved from https://www.reuters.com/article/us-china-zte/u-s-bans-american-companies-from-selling-to-chinese-phone-maker-zte-idUSKBN1HN1P1

United Nations. (2014, January 21). A/RES/68/167. The right to privacy in the digital age. General Assembly. Retrieved from https://undocs.org/A/RES/68/167

Erik Avery, erik.avery@student.sans.edu

United Nations. (2018, October 29). A/C.1/73/L.27/Rev.1 Developments in the field of information and telecommunications in the context of international security. First Committee. Retrieved from https://undocs.org/A/C.1/73/L.27/Rev.1

United Nations. (2018, October 18). A/C.1/73/L.37 Advancing responsible State behaviour in cyberspace in the context of international security. First Committee.

Verizon. (2010). *2009 Data Breach Investigations Report.*

Volz, D. (2017). *Trump administration orders purge of Kaspersky products from U.S. government.* Washington: Reuters. Retrieved from https://www.reuters.com/article/us-usa-security-kaspersky/trump-administration-orders-purge-of-kaspersky-products-from-u-s-government-idUSKCN1BO2CH

Weisman, S. (2008). *Sale of 3Com to Huawei is derailed by U.S. security concerns.* Washington: The New York Times. Retrieved from https://www.nytimes.com/2008/02/21/business/worldbusiness/21iht-3com.1.10258216.html

Erik Avery, erik.avery@student.sans.edu

Appendix A
Global Cyber Protectionist Climate Identification: 2009-2018

Key:

1 - Minimal (Globalist) (0-1)	2 - Developing (2-3)	3 - Moderate (4-5)	4 - Severe (6-7)	5 - Aggressive (Protectionist) 8+

Year	Category	Subcategory	1	2	3	4	5	Annual Climate Rating
2009	Privacy Rights	Data Monitoring Laws	x					2 - Developing
		Data Protection Requirements						
		Intellectual Property Ownership	x					
	Internet Governance	Content-Based Access Restriction						
		Brand/Platform Usage						
		Intra-net Establishment						
	Market Resistance	Product Ban						
		Soft Market Barriers						
		Regulatory Bodies						
2010	Privacy Rights	Data Monitoring Laws						1 - Minimal (Globalist)
		Data Protection Requirements						
		Intellectual Property Ownership						
	Internet Governance	Content-Based Access Restriction						
		Brand/Platform Usage						
		Intra-net Establishment						
	Market Resistance	Product Ban						
		Soft Market Barriers						
		Regulatory Bodies						
2011	Privacy Rights	Data Monitoring Laws						2 - Developing
		Data Protection Requirements						
		Intellectual Property Ownership						
	Internet Governance	Content-Based Access Restriction						
		Brand/Platform Usage						
		Intra-net Establishment						
	Market Resistance	Product Ban						
		Soft Market Barriers						
		Regulatory Bodies	x	x				
2012	Privacy Rights	Data Monitoring Laws	x					2 - Developing
		Data Protection Requirements						

Erik Avery, erik.avery@student.sans.edu

		Intellectual Property Ownership						
	Internet Governance	Content-Based Access Restriction	x					
		Brand/Platform Usage						
		Intra-net Establishment						
	Market Resistance	Product Ban						
		Soft Market Barriers						
		Regulatory Bodies	x					
2013	Privacy Rights	Data Monitoring Laws						**2 - Developing**
		Data Protection Requirements						
		Intellectual Property Ownership						
	Internet Governance	Content-Based Access Restriction						
		Brand/Platform Usage						
		Intra-net Establishment						
	Market Resistance	Product Ban	x	x	x			
		Soft Market Barriers						
		Regulatory Bodies						
2014	Privacy Rights	Data Monitoring Laws						**2 - Developing**
		Data Protection Requirements	x					
		Intellectual Property Ownership	x					
	Internet Governance	Content-Based Access Restriction						
		Brand/Platform Usage						
		Intra-net Establishment	x					
	Market Resistance	Product Ban						
		Soft Market Barriers						
		Regulatory Bodies						
2015	Privacy Rights	Data Monitoring Laws						**2 - Developing**
		Data Protection Requirements						
		Intellectual Property Ownership						
	Internet Governance	Content-Based Access Restriction	x					
		Brand/Platform Usage						
		Intra-net Establishment						
	Market Resistance	Product Ban						
		Soft Market Barriers	x					
		Regulatory Bodies	x					
2016	Privacy Rights	Data Monitoring Laws						**3 - Moderate**
		Data Protection Requirements	x					
		Intellectual Property Ownership						
	Internet Governance	Content-Based Access Restriction						
		Brand/Platform Usage						

Erik Avery, erik.avery@student.sans.edu

		Intra-net Establishment						
	Market Resistance	Product Ban	x					
		Soft Market Barriers						
		Regulatory Bodies	x	x	x			
2017	Privacy Rights	Data Monitoring Laws						**4 - Severe**
		Data Protection Requirements						
		Intellectual Property Ownership	x					
	Internet Governance	Content-Based Access Restriction						
		Brand/Platform Usage	x					
		Intra-net Establishment						
	Market Resistance	Product Ban	x					
		Soft Market Barriers	x					
		Regulatory Bodies	x	x	x			
2018	Privacy Rights	Data Monitoring Laws						**2 - Developing**
		Data Protection Requirements	x					
		Intellectual Property Ownership						
	Internet Governance	Content-Based Access Restriction						
		Brand/Platform Usage						
		Intra-net Establishment						
	Market Resistance	Product Ban						
		Soft Market Barriers						
		Regulatory Bodies	x					

Erik Avery, erik.avery@student.sans.edu

Appendix B
Cyber Protectionist Risk Matrix

	Cyber Protectionist Climate	State of Security	Foreign Organization Relationships	Policy Impact on Industry	Policy Impact on Customer
1	The current cyber protectionist climate is minimal, or globalist. There are virtually no regulations impacting our organization in the areas of assessment based on climate identification. (View specific criteria in Appendix A).	Our organization's state of security is excellent. We have complete, current, and relevant security policies in place, with metrics to prove it. We have industry-accepted frameworks by which to assess our practices and have found no deficiencies in their implementation or adherence. Internal employees conduct security investigations and incident responses while accurately tracking and maintaining security metrics.	We have no relationship with foreign organizations. Our direct customer base, supply chain, and stakeholders share our nationality, and no examination of foreign climates is necessary. We maintain complete ownership of our intellectual property.	There is no impact of protectionist policies on our industry globally. Free-trade and information-based practices are prominent in our organization and among our peers.	Cyber protectionist policies do not influence our customer base. They purchase or receive our goods and services without fear of government intervention. Any regulation does not inhibit our ability to grow our customer base proactively or for more new customers to choose to do business with us.
2	The current cyber protectionist climate is developing. There are two to three policies of concern which direct measures against other industries, but with minimal impact to ours. Political dialogue at the national level suggests intent to formulate more substantial cyber protectionist policies, but they are not imminent and have ambiguous levels of support in government	Our organization's security is comprehensive. 90% of our policies are complete, updated, and relevant to our current business practices. We have a few policies which need redressal. Overall, our security practices are developed and enforced at all levels. We have had only minor security incidents in the past two years and have remediated their root cause.	We have no direct relationships with foreign organizations, but our customers or suppliers may have distant ties. Suppliers may receive some non-critical components from organizations in foreign countries, with no ties to national governments. External organizations seek knowledge about our intellectual property, but disclosure is at	Globalist policies have no impact on our industry but may be impacting others. For the most part, free trade governs our industry with minimal government intervention. Politicians have targeted our organization with more oppressive regulation in the name of national security, but they are years away from being enacted.	Our customers face minor inconveniences from cyber protectionism, but not enough to dissuade their business operations. Policies acting as barriers to our customers are mostly symbolic, do not have a material impact, and are not enforced by governing organizations.

Erik Avery, erik.avery@student.sans.edu

	bodies.		our discretion, and we maintain total ownership and rights.		
3	The current cyber protectionist climate is moderate. There are four or five significant cyber protectionist policies observed globally, which probably have an impact on our organization. These policies restrict the free flow of data in parts of the world, and there is a large number of supporting countries advocating for more restrictions on product and technology proliferation based on nationality.	Our organization's state of security is adequate. We have identified our policy shortfalls and are working on improving our security practices. We have an identified incident response plan and surrounding security policies, but little means of enforcing them. We have suffered a significant number of incidents in the past two years, but do not have the means developed to accurately track investigation and response data.	We have foreign partners with whom we do business, but they do not make up a significant portion of our market base or supply chain. There are no direct ties with foreign governments and these partners, but foreign governments have expressed interest in regulating our business agreements.	Some protectionist policies target our industry, but they do not heavily restrict our capability to do business. Policies are enacted against our industry but are only enforced in extreme cases. Governments are seeking additional policies, but they are not aggressively seeking to hamper industry activities across borders.	Cyber protectionist policies moderately inconvenience our customers. They encounter moderate resistance from their government in order to do business with us, but overall, are still capable of doing so if they desire. Their inconvenience is enough to drive away a portion of our new customers, but many of them believe that the administrative hurdles are acceptable.
4	The current cyber protectionist climate is severe. There are six or seven national or global policies hampering free-trade and flow of information. Global ideologies are trending on nationalistic, with the large scale banning of products and wide-reaching legislation on tight internet governance laws. Globalist ideologies are shrinking, and	Our organization's state of security is emerging. We have dated policies in place which are no longer relevant to our current business operations. We know we have suffered significant breaches in the past two years and have had to hire external security professionals on a routine basis to remediate our incidents.	A significant portion of our external partners remains foreign. Some may have ties to foreign governments but maintain their status as respected private organizations. The foreign government maintains strict control over our business relationship.	Our industry is regulated by global cyber protectionist policies. We are restricted from much of the global market based on heavy regulation targeting the expansion of our industry in foreign nations. National governments and market authorities enforce policies over markets in which we desire to operate.	Our customers are severely restricted by protectionist policies. They are not legally allowed to conduct business with us, but either the government cannot actively enforce their regulations, or customers are bypassing them through the use of third parties or technology-based capabilities.

	political dialogue continues to press from more sweeping action and restrictions in the name of security.				
5	The current cyber protectionist climate is aggressive. There are at least eight identified protectionist policies or actions which significantly impact our organization. Global political bodies aggressively pursue and adopt new legislation and executive action to restrict our organization's access to global markets or explicitly block others from engaging with us. Cross-border data transactions are severely restricted or entirely prohibited.	Our organization's state of security is inadequate. We have virtually no security policies in place and no means of enforcing them. User awareness of threats is probably minimal, and we do not know what incidents have occurred.	A large portion of our external partners resides in foreign countries, or with foreign country governments. Foreign governments require complete surrender of our intellectual property and require extensive national security investigations before entering their markets.	Cyber protectionist policies heavily regulate our industry. Organizational growth is hampered by policies which directly require government intervention in our development of new services based on our industry classification.	Cyber protectionist policies aggressively restrict our customers. Global and nation policies restrict their ability to purchase goods and services from our organization and there are no means of bypass.

Erik Avery, erik.avery@student.sans.edu

Appendix C
Appendix C – Risk Discovery Worksheet

To accurately predict the threat to the organization based on the identified cyber protectionist criteria, use the results from the Cyber Protectionist Risk Matrix to fill in the blanks below. The overall score will place it in a threat category, from which the overall risk to the organization is identified.

Criteria	**Score:**
1. Cyber Protectionist Climate	
2. State of Security	
3. Foreign Organization Relationships	
4. Policy Impact on Industry	
5. Policy Impact on Customer	

Total: _____

Risk Level Assessment:

5: NEGLIGIBLE	6-10: LOW	11-15: MODERATE	16-20: HIGH	20-25: CRITICAL

Erik Avery, erik.avery@student.sans.edu

Last Updated: September 20th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS San Francisco Fall 2019	San Francisco, CAUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Dallas Fall 2019	Dallas, TXUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS London September 2019	London, GB	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Kuwait September 2019	Salmiya, KW	Sep 28, 2019 - Oct 03, 2019	Live Event
SANS Tokyo Autumn 2019	Tokyo, JP	Sep 30, 2019 - Oct 12, 2019	Live Event
SANS Cardiff September 2019	Cardiff, GB	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS Northern VA Fall- Reston 2019	Reston, VAUS	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS DFIR Europe Summit & Training 2019 - Prague Edition	Prague, CZ	Sep 30, 2019 - Oct 06, 2019	Live Event
Threat Hunting & Incident Response Summit & Training 2019	New Orleans, LAUS	Sep 30, 2019 - Oct 07, 2019	Live Event
SANS Riyadh October 2019	Riyadh, SA	Oct 05, 2019 - Oct 10, 2019	Live Event
SANS Baltimore Fall 2019	Baltimore, MDUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS October Singapore 2019	Singapore, SG	Oct 07, 2019 - Oct 26, 2019	Live Event
SANS Lisbon October 2019	Lisbon, PT	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS San Diego 2019	San Diego, CAUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SIEM Summit & Training 2019	Chicago, ILUS	Oct 07, 2019 - Oct 14, 2019	Live Event
SANS Doha October 2019	Doha, QA	Oct 12, 2019 - Oct 17, 2019	Live Event
SANS Seattle Fall 2019	Seattle, WAUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS SEC504 Madrid October 2019 (in Spanish)	Madrid, ES	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Denver 2019	Denver, COUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS London October 2019	London, GB	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Cairo October 2019	Cairo, EG	Oct 19, 2019 - Oct 24, 2019	Live Event
SANS Santa Monica 2019	Santa Monica, CAUS	Oct 21, 2019 - Oct 26, 2019	Live Event
Purple Team Summit & Training 2019	Las Colinas, TXUS	Oct 21, 2019 - Oct 28, 2019	Live Event
SANS Training at Wild West Hackin Fest	Deadwood, SDUS	Oct 22, 2019 - Oct 23, 2019	Live Event
SANS Orlando 2019	Orlando, FLUS	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS Houston 2019	Houston, TXUS	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS Amsterdam October 2019	Amsterdam, NL	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS DFIRCON 2019	Coral Gables, FLUS	Nov 04, 2019 - Nov 09, 2019	Live Event
Cloud & DevOps Security Summit & Training 2019	Denver, COUS	Nov 04, 2019 - Nov 11, 2019	Live Event
SANS Paris November 2019	Paris, FR	Nov 04, 2019 - Nov 09, 2019	Live Event
SANS Sydney 2019	Sydney, AU	Nov 04, 2019 - Nov 23, 2019	Live Event
SANS Mumbai 2019	Mumbai, IN	Nov 04, 2019 - Nov 09, 2019	Live Event
SANS Bahrain September 2019	OnlineBH	Sep 21, 2019 - Sep 26, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced