Red Teaming Analysis of a Widespread Catastrophic Cyber Incident
An Expert Panel Discussion

Catastrophe and Climate

PART 3

MAY | 2023

SOA Research INSTITUTE

Red Teaming Analysis of a Widespread Catastrophic Cyber Incident

An Expert Panel Discussion

AUTHORS Unal Tatar, PhD
Brian Nussbaum, PhD
Omer F. Keskin, PhD
Doug Clifford
Elisabeth Dubois, MBA, PMP
Dominick Foti, MBA
Brianna Bace
Rian Davis

SPONSOR Catastrophe and Climate Strategic Research Program Steering Committee

Casualty Actuarial Society

CONTENTS

Red Teaming Analysis of a Widespread Catastrophic Cyber Incident

An Expert Panel Discussion

Executive Summary

The increasing reliance on technology and digital infrastructure has led to the emergence of software supply chain vulnerabilities as one of the most significant threats to organizations across various sectors. The objective of this report is to identify potential vulnerabilities in the insurance sector and explore the impact of a software supply chain vulnerability on the insurance industry.

This report is the third deliverable of a series of four expert panel discussions on catastrophic cyber incidents. The report presents the findings of the March 2023 expert panel meeting where the participants conducted a red teaming exercise and discussed a hypothetical catastrophic cyber incident that was caused by a software supply chain vulnerability and spread to over three thousand organizations around the world across all sectors.

The expert panel discussion answered several research questions about the biggest risks and challenges for the insurance sector to respond to such developing cyber incidents, the course of action of the insurance industry, and how the insurance companies could react to reduce the risk of not yet targeted clients. The report provides a detailed account of the methodology and outcomes of the expert panel convened for a two-hour session. The panel utilized the Red Teaming Methodology, which is a commonly used methodology in policy and security circles, to elicit insights regarding catastrophic cyber risks.

The conclusions drawn from the conversations reveal information about the impact of the incidents and challenges for the insurance industry. The panelists suggest that insurers need to ensure they have the necessary resources in place to respond quickly and effectively to claims, including IT forensics vendors, breach coaches, and other third-party providers. Tabletop exercises with both C-Suite representatives and IT teams are recommended to be conducted.

The panelists also emphasized the importance of communication and collaboration between insurers, businesses, and the government in the event of a cyber-attack. Effective communication is crucial in ensuring that all parties are on the same page and can work together to address the challenges of a cyber-attack. The discussion highlights the need for insurers to be proactive in reaching out to their clients to ensure they are doing all they can do to prevent being victimized by cyber-attacks. The report also highlights the challenges associated with information sharing and liability in the cybersecurity insurance industry. The issue of complicated ownership was raised, with questions of who would be responsible for liability in cases where multiple parties were involved. The panelists concluded that there needs to be a framework to encourage data sharing among companies, insurers, and regulators, and the government's involvement would be key in determining how fast and efficiently vulnerabilities are addressed.

Section 1: Introduction

The cyber landscape has been evolving rapidly with the increasing reliance on technology and digital infrastructure. As the world becomes more connected, the risks associated with cyber threats are escalating at an unprecedented rate. In particular, software supply chain vulnerabilities have emerged as one of the most significant threats to organizations across various sectors. These vulnerabilities can be exploited by cybercriminals to infiltrate and compromise critical systems, resulting in catastrophic consequences.

Catastrophic cyber risks can be defined as the risks that impact "the quality of life for a large number of people, impact the confidentially, integrity, and availability of information, or causes a wide-scale business interruption"[1]. Catastrophic cyber risks are critical due to the challenges of estimating the likelihood and impact compared to the traditional risk events the insurance companies are used to handling. A rapidly spreading threat across thousands of victim organizations would cause a widespread impact across sectors. Considering such catastrophic risks from various aspects require a multi-disciplinary approach. Therefore, it's essential to gather insights from a diverse range of experts across various sectors. This project aims to organize a series of panel discussions utilizing the red teaming technique, involving experts from the insurance industry, government, private sector, and academia. The objective is to obtain feedback on the current and emerging catastrophic cyber risks and to identify strategies for mitigating them through a multi-disciplinary approach.

To better understand the impact of a rapidly spreading cyber-attack scenario on the insurance sector, a red teaming exercise was conducted where participants played the role of the cyber insurance sector. The exercise aimed to identify potential vulnerabilities in the insurance sector and explore the impact of a software supply chain vulnerability on the cyber insurance industry. The exercise provided valuable insights into the potential impact of such an incident and highlighted the need for insurance companies to be better prepared to respond to these types of events.

This report is the third deliverable of a series of four expert panel discussions on catastrophic cyber incidents.

The first report[1] is based on the October 2022 expert panel meeting and attempted to synthesize the definitions of catastrophic cyber risks, how these risks are addressed, and the challenges the insurance industry faces. It also established a framework for the upcoming red teaming exercises of the project.

The second report[2] is based on the January 2023 expert panel meeting and presented the outcomes of the first red teaming exercise for a catastrophic cyber incident that targets a critical infrastructure sector, transportation, and how the ripple effects would impact the insurance industry and the whole economy. Discussions regarding the coordinated cyber-attacks along with a major hurricane that impacts multiple major U.S. ports were delivered with this report.

This report is based on the March 2023 expert panel meeting where the participants conducted another red teaming exercise and discussed a catastrophic cyber incident that is caused by a software supply chain vulnerability and spread to over three thousand organizations around the world across all sectors.

---

[1] Tatar, U., Nussbaum, B., Keskin, O. F., Dubois, E. V., & Foti, D. (2022). *Setting the Scene: Framing Catastrophic Cyber Risk An Expert Panel Discussion* (Catastrophic Cyber Risk: An Expert Panel Discussion Series). Society of Actuaries. https://www.soa.org/resources/research-reports/2023/cat-cyber-risk/

[2] Tatar, U., Nussbaum, B., Keskin, O. F., Clifford, D. C., Dubois, E. V., Foti, D., Bace, B., & Davis, R. (2023). *Red Teaming Analysis of a Catastrophic Cyber Attack on Critical Infrastructure An Expert Panel Discussion* (Catastrophic Cyber Risk: An Expert Panel Discussion Series). Society of Actuaries. https://www.soa.org/resources/research-reports/2023/cat-cyber-risk/

The objective of this panel discussion was to answer the question: "What are the potential impacts of a catastrophic cyber incident on the insurance industry, economy, and the nation?" To elaborate this question, several research questions regarding a catastrophic cyber incident were stipulated:

- What are the biggest risks and challenges for the insurance sector to respond to such developing cyber incidents and how to overcome these challenges?
- What is the course of action of the insurance industry?
- What would the insurance companies' reaction be to reduce the risk of not yet targeted clients?
- How can the insurance sector prepare for such a scenario?

The contents of this document provide a detailed account of the methodology and outcomes of an expert panel convened for a two-hour session. To promote transparency and encourage candid discussions, participants were assured that no ideas were attributed to any individual or company in this report. Rather, the report's focus is on summarizing the ideas and opinions shared during the panel discussion. However, the Acknowledgements Section does include the names of all participants who contributed to the discussion.

Section 2: Methodology

2.1 RED TEAMING

This project adopts the methodology of red teaming, which is a commonly used methodology in policy and security circles, to elicit insights regarding catastrophic cyber risks. More information about the Red Teaming Methodology can be found in the second report of this series.[3] The expert panel in the meeting has been provided with a catastrophic cyber incident scenario and invited for debriefing. The core scenario has been updated with two "injects" (fictional events or developments) to structure a discussion about how risk management processes might play out and perspectives can change. The two-hour tabletop exercise was based on scenarios and topics published in the first report[4] and the outcomes of the second report[3] of this project.

2.2 SCENARIO & INJECTS

The scenario in the exercise is a developing cyber incident where the role players first have an initial insight into the preliminary symptoms of the widespread cyber-attack. The core scenario was shared with participants as a read-ahead narrative. After discussing the current situation and the initial response of the cyber insurance industry, the first inject is provided by giving additional details about the incident that are revealed during a week. The reactions and the changes in the response of the insurance sector were discussed. Finally, the second inject was provided with more emergent news regarding the incident and changing threat landscape. This was followed by the final discussion on how the insurance sector would be affected. The scenario and injects are briefly discussed in the following subsections and provided as-is in the Appendices.

---

[3] Tatar, U., Nussbaum, B., Keskin, O. F., Clifford, D. C., Dubois, E. V., Foti, D., Bace, B., & Davis, R. (2023). *Red Teaming Analysis of a Catastrophic Cyber Attack on Critical Infrastructure An Expert Panel Discussion* (Catastrophic Cyber Risk: An Expert Panel Discussion Series). Society of Actuaries. https://www.soa.org/resources/research-reports/2023/cat-cyber-risk/

[4] Tatar, U., Nussbaum, B., Keskin, O. F., Dubois, E. V., & Foti, D. (2022). *Setting the Scene: Framing Catastrophic Cyber Risk An Expert Panel Discussion (Catastrophic Cyber Risk: An Expert Panel Discussion Series). Society of Actuaries.* https://www.soa.org/resources/research-reports/2023/cat-cyber-risk/

2.2.1 EXERCISE CREATION

The cyber incident scenario for this exercise was developed based on the feedback from the first two expert panel meetings. The scenario is intended to be a widespread, high-impact, and low-probability scenario. Although such a catastrophic incident has not yet happened, there is no guarantee that it will never occur in the near future. Since the main focus for this scenario is to be a widespread one, the project team have determined the attack vector to be a software supply chain. Some software products are used by almost all companies globally. In case there is an effective intrusion method spread through the software supply chain to all users, e.g., providing remote access to malicious actors, the scenario can easily become a catastrophic incident depending on the ambition, motivation, and experience of the threat actors. This would cause a sector-agnostic incident where organizations from almost all sectors can become a victim, leading to possible consequences on various aspects of the spectrum. During hypothetical scenario creation, real incidents (SolarWinds,[5] NotPetya,[6] Log4j,[7] and Heartbleed[8]), hypothetical cyber incident scenarios[9,10,11] and other relevant documents by the government and other organizations[12,13] were utilized.

The scenario initializes with the news of several high-profile data breach incidents reported over a week. The initial forensic investigations by victim organizations, which are not directly related to each other, realize a possible supply chain compromise that is tied to the database management tool called DataVex. The piece of software is ubiquitously used by organizations around the world. The threat intel report accompanied in the core scenario read ahead indicates an organized crime group has been attacking the vendor of DataVex for the last five months. It is also indicated that the initial data breaches focus on stealing Personally Identifiable Information (PII) and Personal Financial Information (PFI) held by dozens of companies from various sectors. The estimates of aggregated losses by organization size were adapted from the study conducted by Lloyd's and Cyence.[11] Figure 1 provides a synopsis of the inputs provided to the panelists with each phase of the scenario.

[5] FireEye. (2020). *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor*. Mandiant. https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

[6] Greenberg, A. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[7] Cyber Safety Review Board. (2022). *Review of the December 2021 Log4j Event*. https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf

[8] Fruhlinger, J. (2022, September 6). *The Heartbleed bug: How a flaw in OpenSSL caused a security crisis*. CSO Online. https://www.csoonline.com/article/3223203/the-heartbleed-bug-how-a-flaw-in-openssl-caused-a-security-crisis.html

[9] Cambridge Centre for Risk Studies, Lloyd's of London, & Nanyang Technological University. (2019). *Bashe Attack: Global Infection by Contagious Malware*.

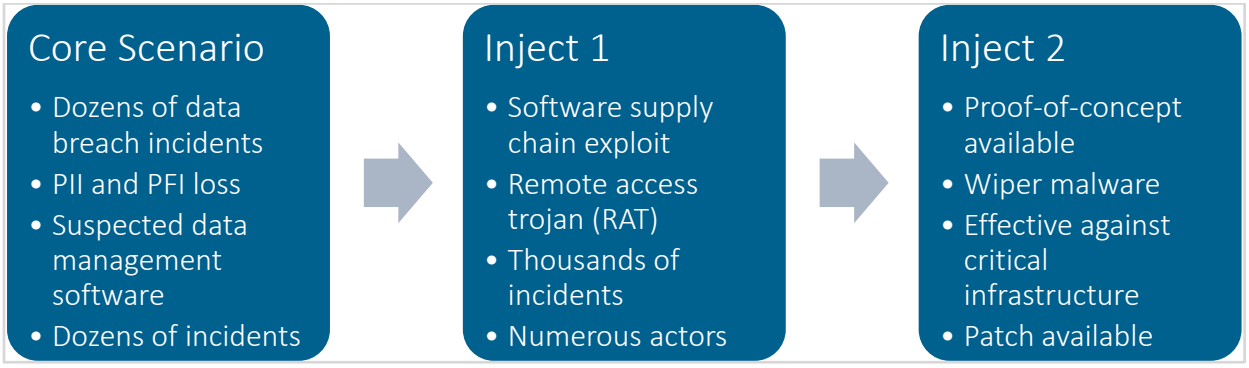
[10] Lloyd's of London, Cambridge Centre for Risk Studies, & Nanyang Technological University. (2019). *Shen attack Cyber risk in Asia Pacific ports*.

[11] Lloyd's & Cyence. (2017). *Counting the Cost—Cyber Exposure Decoded* (Emerging Risk Report).

[12] American Property Casualty Insurance, Association The Council of Insurance Agents and Brokers, CyberAcuView, & The Wholesale & Specialty Insurance Association. (2022). *Re: Potential Federal Insurance Response to Catastrophic Cyber Incidents*.

[13] US Government Accountability Office. (2022). *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks* (GAO-22-104256; Report to Congressional Committees).

Figure 1
SUMMARY OF INPUTS IN THE CORE SCENARIO AND TWO INJECTS



2.2.2 CORE SCENARIO

The core scenario consists of two pieces: a news article and a threat intelligence note.

According to the news article, a new wave of data breaches has been reported in recent days affecting dozens of companies across different industries and sectors, resulting in the loss or potential loss of personally identifiable information (PII), including credit card information. Although there's no obvious pattern yet, some people tied to cyber incident response firms suggest that a common software vulnerability may be responsible for the attacks. Speculations in the cybersecurity industry suggest that the widely used software DataVex, a database management tool, could be the common link among the targeted companies. The impact of such a supply chain compromise on DataVex could be catastrophic since it is deployed by hundreds of thousands of organizations globally.

The second report is a warning message from Securitonin, a threat intelligence company, to its customers about the data breach incidents related to the software DataVex. It appears that at least one known organized crime group, Static Harpsichord (SH), has been attacking this software for months. SH may have purchased this vulnerability or access on a malware-focused auction site last summer. The data breach incidents resulted in the compromise of confidential data, such as SSNs, credit and debit card information, trade secrets, and intellectual property. Most of Securitonin's clients that run DataVex on their systems have artifacts or activity suggesting the presence of SH or a potential compromise tied to this vulnerability. Securitonin advises clients who run DataVex to reach out immediately for mitigation and response support.

2.2.3 INJECT 1: INTEL UPDATE 1

According to the intel update, the cause of the data breach incidents was identified as a software supply chain exploit that leveraged the software update process of DataVex. The malware has been identified as a remote access trojan (RAT) which allows attackers to easily control the infected systems and spread into the internal network of the victim organization. The RAT was initially used by one cybercriminal group to exfiltrate sensitive data from over 1600 companies, but it has now been sold on the dark web to other interested hacker groups. There are now numerous cybercriminal crews using the DataVex access vector to access a wide variety of corporate and government information technology environments, stealing Personally Identifiable Information (PII) / Personal Financial Information (PFI) / Protected Health Information (PHI), stealing intellectual property and trade secrets, and conducting ransomware attacks. The update presents the estimated losses based on the currently reported incidents, with the total estimated losses being $37.7bn. However, this number may still increase significantly considering the number of organizations that deployed DataVex.

2.2.4 INJECT 2: INTEL UPDATE 2

The second intel update provides new developments on the DataVex vulnerability. A proof-of-concept (POC) code for exploiting it has been posted online, resulting in an explosion of attacks on networks running DataVex. Many companies have attempted to remove DataVex from their systems, but this has often happened too late.

One of the most serious developments is the release of an easy-to-use wiper malware called "DataVeccS", which reportedly destroyed large amounts of data on some networks where it has been deployed. The wiper malware is also effective against Industrial Control System networks, causing disruption in critical infrastructure sectors.

DataVex has announced that they will publish a patch today, but it is unclear how effective it will be in removing the RAT from infected systems and how quickly organizations around the world will be able to apply the patch. The update also provides loss estimates for organizations based on currently reported incidents, which show the expected losses of $52.6 billion, with a 95% confidence interval of $41.22bn to $63.98bn.

ROLES & DISCUSSION QUESTIONS

During the red teaming exercise, participants played the role of the cyber insurance sector to reveal the potential impact on the insurance sector due to such a catastrophic incident caused by a software supply chain vulnerability. By assuming the role of the cyber insurance sector, the participants aimed to identify potential risks, challenges, possible reactions, and losses associated with the incident and to minimize the losses for insurers caused by the overall incident.

Section 3: Findings

3.1 INCIDENT RESPONSE

3.1.1 VULNERABILITIES & THREAT ACTORS

The insurance industry faces a growing threat from cyber-attacks, particularly in the wake of supply chain vulnerabilities such as the Log4J exploit and SolarWinds incident. One major concern raised by the panelists representing the insurance industry was the interconnectedness and complexity of the modern supply chain ecosystem, which makes catastrophic cyber supply chain incidents realistic and probable. In this scenario, anyone could be a victim, including the insurers themselves. This could lead to attackers stealing personally identifiable information (PII) from insurance companies for monetary gain, making them a prime target.

If insurers were compromised, they could become a vector for attacking their clients. For example, attackers could use a response mechanism to reach out to clients and provide them with instructions on how to prevent being compromised. Since clients trust their insurers, they are likely to follow the instructions, which could further escalate the attack.

However, the motivation of the attackers may not always be what it appears. While it seems they are stealing data for monetary gain, they could also be trying to gain access to information that allows them to compromise industrial control systems. This raises the question of whether attackers are gaining access to information that would allow them to shut down or take control of critical infrastructure.

There was considerable debate among panelists about whether insurance companies should focus on big businesses with annual revenue of $1 billion or higher, or small and medium-sized businesses (SMBs) that span across the

insurance spectrum with different carriers. Some argued that insurers should focus on big businesses, as their losses are catastrophic, while others believed that SMBs are more vulnerable and thus more deserving of attention.

Vulnerabilities are exploitable, not because they exist, but because attackers can exploit them. In many cases, experts shared how adversaries will gain an initial foothold and then maintain persistence to cause damage at a later point in time. Therefore, it is important for insurers to identify and address vulnerabilities proactively to prevent attacks.

3.1.2 PREPARATION

The panel discussion provided insights into incident response and preparation for a catastrophic cyber event. The recent Log4J exploit highlighted the need for comprehensive and effective risk management strategies, especially in addressing supply chain vulnerabilities. The lack of claims adjusters and services can pose challenges for insurers, particularly when triaging customers in the aftermath of a cyber-attack. The panelists suggest that insurers need to ensure they have the necessary resources in place to respond quickly and effectively to claims. These services could include IT forensics vendors, breach coaches, and other third-party providers.

Some cyber insurers are using external security scans to identify compromised systems and provide clients with the third-party services, including providing information and guidance they need to respond effectively. However, insurers also need to be flexible and allow for client-specific responses to meet the unique challenges of each situation. It is vital to have tabletop exercises, so entities are prepared, know what resources are available, and how to address a catastrophic cyber event. Recovery is faster and less expensive if they have a plan in place.

The discussion highlights the importance of collaboration, communication, and tabletop exercises in preparedness for a catastrophic cyber event. Insurers need to develop comprehensive risk management strategies that consider the unique challenges of each situation and provide their clients with the support and resources they need to respond effectively. Effective communication and collaboration are key to success in this area.

The increasing complexity and interdependence of the software supply chain, coupled with the rising sophistication of cyberattacks, means that the risk of a catastrophic cyber supply chain incident is significant and should be taken seriously by businesses and governments alike. It is important for organizations to take proactive steps to secure their supply chain, including conducting regular risk assessments, implementing robust security protocols, and establishing strong partnerships with trusted suppliers and service providers.

The liability for software development is challenging, and, although identified as a strategic objective in the latest U.S. National Cybersecurity Strategy[14] released in March 2023 (i.e., Shift liability for insecure software products and services), there is no widely accepted method to hold software vendors accountable for vulnerabilities in their products. However, this can push companies to improve their cybersecurity measures and hold vendors accountable for their products' security. The adoption of cloud-based models can pose new risks, and insurance companies need to reassess their policies to address emerging risks.

One of the most important takeaways of the discussion is the importance of preparation and mitigation of cyber-attacks. In the event of an attack, companies that know what resources are available, how to access them, and how to prevent catastrophic damage to their business and clients are in a much better place than those who do not

[14] The White House. (2023). *U.S. National Cybersecurity Strategy released in March 2023*. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

know this information. Tabletop exercises with both C-Suite representatives and IT teams are recommended to be best prepared.

The discussion also highlighted the need for insurers to be proactive in reaching out to their clients to ensure they are doing all they can to prevent being victimized by cyber-attacks. Companies that have cybersecurity insurance coverage should be aware of the types of coverage triggered by a cyber-attack, including cyber event response, privacy liability, and technology errors and omissions. The panelists also recommended that insurers collaborate to develop a standard for cyber insurance policies that ensures that companies meet specific criteria to reduce the likelihood of cyber incidents.

3.1.3 TRIAGE & EXPOSURE

Based on the discussions by panelists, the insurance industry faces significant risks given supply chain vulnerabilities. In such situations, insurers must be concerned with getting the right information out there, including the number of clients that will be impacted, the risks involved, and whether the incident will be catastrophic. Insurers also want to know the level of their exposure, particularly since most forensics are remote. Replacement hardware may become an issue, and there is a lack of visibility in determining how bad an incident is going to be.

The lack of claims adjusters and services, as well as the ability of insurers to triage for customers, presents a challenge. Security professionals may not be well-versed in the event to help, and there may not be enough experts in third parties to assist businesses and the economy in the case of a widespread loss.

There is a concern about how insurers will prioritize clients if there is a significant loss in terms of critical infrastructure, payments, and so on. This will vary from company to company, and insurers will have to consider whether to prioritize clients based on relationship, profit, or government intervention plan. This is an example of where most current tabletop exercises fall short. They typically do not adequately consider the potential for cascading failures due to systems and resources that work under normal load but would fail (without emergency planning) when put under increased stress.

In the event of such an attack, insurers have a duty of care to cover all companies, both small and large. The solvency of insurance companies is a concern, and the CEOs focus on their own clients first. Regulators will likely be involved, determining the exposure and what is being done to mitigate the largest risks.

In the event of an attack that goes beyond a loss of data and leads to a loss of life, panelists share how the purpose and use of the information should be considered.

The risks and challenges related to Industrial Control Systems (ICS) also require consideration, as ICS brings in a different type of response, and Cybersecurity and Infrastructure Security Agency (CISA) would certainly get involved, and based on the case, Federal Emergency Management Agency (FEMA) may also get involved in the response to ICS incidents. There is a need for a comprehensive response plan that considers the unique nature of ICS incidents.

In such an attack, insurers do not know if their client uses the software or if they have the version of the software with the vulnerability. Insurers also may not know if the defense their clients employ is strong enough to prevent attackers from exploiting the vulnerability, whether there is a patch for the vulnerability, and how long it takes to apply the patch. These unknowns complicate the response process. Though it is not common that insurance companies will contact every client in the portfolio, some[15] does continuously monitor for these exposures and does

[15] https://cyrisk.com/

outreach to all affected policyholders on behalf of the carriers. Carriers can also disseminate more general information through mass media chains.

The insurance industry as a whole has become much better positioned to address cybersecurity challenges in the last couple of years. The current process for granting cyber coverage is much more involved than it has been in the past, with a shift away from relying on simple questionnaires and towards more actionable checking mechanisms such as requiring implementation of multi-factor authentication. This has aided in alleviating some of the insurer's risks, though not completely. On the other hand, the increased competition occurring today in the cyber insurance market has unfortunately led some carriers to lower their underwriting standards in an effort to win the business. This will undoubtedly lead to a return to increasing claims and worsening loss ratios again.

Panelists share how insurance companies can prepare for potentially disastrous incidents by conducting realistic disaster scenarios and modeling, reviewing portfolios, and correlating exposures. In terms of financial and accumulation management, insurance companies are also protecting themselves from losses with more robust underwriting guidelines before providing cyber insurance.

If the vulnerable database system (i.e., DataVex) was externally facing, insurance companies might be able to detect this application within their clients. This would allow them to develop a targeted response. Insurance companies may allow the affected companies to select their own incident response vendors so that panel vendors are not exclusively relied upon. Many of the same incident response vendors are on multiple insurance carrier approved vendor panels. This over-reliance on a small number of vendors could become another systemic failure during a catastrophic event, compounding incident costs if business outages are extended due to a shortage of approved incident response resources.

3.1.4 RESOURCE ALLOCATION

The panel discussed incident response and resource allocation. One panelist pointed out that focusing only on large companies could result in class action lawsuits from smaller entities, and insurers need to be prepared to handle sector-specific regulatory investigations at the federal and state attorney general level.

The panelists agreed that understanding where the greatest exposure is and how to mitigate it would be a top priority. However, there was some disagreement over client prioritization. One panelist argued that although small businesses would be impacted the most, insurers should focus on larger companies where the most loss is concentrated. The evolving nature of the scenario would also influence prioritization. Likewise, another panelist referred to a chart from inject 1 and recommended that insurers focus on larger organizations to minimize losses.

Another expert disagreed and argued that small/medium businesses would be a greater concern since they are less likely to have the threat intelligence and other security resources to get ahead of the exposure. In addition, like the spread of COVID, the greater the population of infected hosts, the greater the risk of further contagion to other policyholders hence a higher aggregated loss for the insureds. They argued that cyber insurance has become a duty of care coverage for most companies regardless of size, and that many small companies would have some form of coverage. Moreover, focusing only on larger companies could trigger class action lawsuits and attract attention from governmental directives about company prioritizations.

3.1.5 RESPONSE & SUPPORT

The panelists in this discussion on incident response and support agreed that insurance customers expect support teams to be available to assist with the aftermath of a cyber-attack. However, the question of what happens next arises when patches are not available, or vulnerabilities remain open. Insurers may put clients in touch with third-party providers, but this creates challenges in identifying suitable vendors and coordinating their efforts. Insufficient

capacity to conduct forensics or other constraints on response capacity may require government intervention or response.

Panelists proposed that insurers should not focus on individual companies but should instead provide an equitably scaled response in the event of a large-scale scenario. Meanwhile, the introduction of wiper cases introduces new risks and challenges, which could lead to potential shifts in response and collaboration. Government involvement and response would be sparked by economic implications and public pressure. Moreover, the difficulty of patching ICS and provisioning replacement hardware/equipment in the case of wipers could limit insurers' ability to provide support to all clients.

One panelist notes that self-insured retention limits are exceeded, insurance companies will respond with resources. Typically, incident response resources are provided immediately, and who pays when may differ on a policy-by-policy basis. Many policies offer first dollar coverage for breach coaches. However, they believe that the insurance company would not be able to provide enough support teams, and cyber services are not scalable. Another relates this situation to the Log4J zero-day, where the majority of patching was conducted by IT professionals, not security professionals.

3.1.6 RISKS & CHALLENGES

Various avenues of the discussion expanded on risks and challenges in responding to the incident. One major challenge panelists raised is the lack of visibility into the extent and severity of the attack, making it difficult for insurers to respond effectively. For example, many in the insurance industry though Log4Shell was going to cause massive loss accumulation, but thus far, it has barely registered. The accumulation risk is tough to measure and manage in the cyber insurance industry.

The discussion also touches on the impact of cyber-attacks on industrial control systems (ICS), where FEMA may get involved, and the risk may not diminish over time. Large syndicates are required to do Realistic Disaster Scenario (RDS) modeling[16], and the third-party services provided with cyber insurance are scalable. However, there may not be enough adjusters or response partners to react to problems in such specialized environments.

Regarding the second inject, insurance companies may review warranty statements to determine whether clients were forthright. However, proving material misrepresentation would be difficult with such a large-scale event. Insurance regulators or government offices may declare that insurers must provide coverage regardless of warranty statements or misrepresentation. Still, a desire to preserve reputation may prompt insurers to cover the claims.

Panelists also discuss how if the insured loss is in the tens of billions of dollars, new insurance may not be written for organizations.

3.1.7 CAPACITY

The panelists highlight concerns about incident response capacity in the event of a catastrophic cyber-attack on the supply chain. The shortage of resources, including personnel, could cause bottlenecks as everyone is looking for the same services at the same time. To address this, the panelists suggest that companies be flexible and adaptable to changing circumstances, and people in different positions could be reused to help with the bottlenecking.

[16] https://www.lloyds.com/conducting-business/underwriting/realistic-disaster-scenarios

The importance of proactive risk management measures, such as timely patching and vulnerability management, is emphasized. The exposure of this scenario would be long-lasting, as even after patches are introduced, there will be activity spikes caused by persistent actors already present in the systems.

Capacity and bandwidth issues may arise, and there could be a shortage of security experts to address the immediate needs of the affected companies. This would be exacerbated by any attack on ICS since there are far fewer security or IT professionals who are capable of working with these systems. The solution to this problem may lie in utilizing people from smaller IT roles or tertiary providers, but this may not be enough to address the scale of the problem.

There is also a discussion of capacity in relation to modeling and third-party companies for IT forensics. The panelists suggest that there may not be enough security experts if there is a larger outage across multiple industries, and there are often no hard and fast rules for remediation activities. The panelists emphasize the importance of proactive risk management and the potential challenges that may arise in the event of a catastrophic cyber-attack on the software supply chain.

3.2 RISK REDUCTION & INFORMATION SHARING

3.2.1 INFORMATION SHARING

According to the panelists, the insurance industry plays a critical role in mitigating the risks and reducing the impact on customers during a supply chain vulnerability. Insurers are expected to provide support and guidance to their customers, and they can rely on third-party companies and information sharing to accomplish this goal. Cyber-attacks pose a significant threat to the insurance industry, and it is essential to remain vigilant and proactive in protecting their customers. The panelists highlighted the importance of communication and collaboration between insurers, businesses, and the government in the event of a cyber-attack. Effective communication is crucial in ensuring that all parties are on the same page and can work together to address the challenges of a cyber-attack. It is also essential for insurers to provide support and guidance to their customers, and they can rely on third-party companies and information sharing to accomplish this goal.

Insurers may also post information from the Cybersecurity and Infrastructure Security Agency (CISA) and other relevant sources or share a bulletin about risks to watch. This information can help customers stay informed about the latest developments in cybersecurity and take steps to protect themselves. However, the response of insurers may differ depending on the type of attack. For instance, supply chain compromises may be viewed differently than zero-day exploits, and insurers may rely on third-party companies that are well-versed in the event to help. Communication challenges between insurers, clients, brokers, and legal counsel can present further issues for insurers. Collaboration and communication will play a key role in the response to minimize losses.

Insurers of varying sizes will offer different services, and detailed risk assessments and scans for all cyber insurance lines will be essential. One of the challenges faced by insurers is data sharing, which is essential for them to make informed decisions about their policyholders' cybersecurity posture. However, data sharing remains a challenge due to companies' unwillingness to share information about their security measures and breach incidents. This highlights the need for a framework to encourage data sharing among companies, insurers, and regulators.

According to the panelists, another important consideration is the scale of the response. Instead of focusing on individual companies, there should be a focus on scaling the response. For example, if there is a weakness in the update process of popular software, the first thing to do is to get this information out to all clients. It is important to work with other companies and government agencies to share the information at scale. In an incident of this size, regulators would certainly be reaching out to ask for information regarding exposure, best-case, and worst-case scenarios. Regulatory investigations focusing on the amount of personally identifiable information released will also

be launched, with the type of investigation being dependent on which sector has been impacted. Detection and patching alone will not be sufficient to solve the problem. A forensic analysis is necessary to determine whether or not there as already been a compromise and threat actors have gained a foothold inside the policyholder's network. If the results of the investigation indicate there has been, the course of action will shift.

3.2.2 RESOURCES & GOVERNMENT INVOLVEMENT

The panelists discussed the potential impact of cyber-attacks on insurers and the need for detailed risk assessments and scans for all cyber insurance lines. They acknowledged that in the event of a widespread attack, there may not be enough experts in third parties to assist businesses and the economy. This is where the government may intervene by deploying resources to support the response of companies deemed to play a significant role in critical infrastructure. There may be some challenges here in coordinating the response, but CISA provided extremely useful information to assist in the response, without stepping on the toes of insurance company or policyholder resources.

The panelists also discussed the impact of wiper cases on the availability of hardware. This was best exemplified by the Maersk NotPetya case where they had to provision many thousands of laptops. It was challenging when the incident occurred and would most likely be even more challenging given today's technology supply chain issues. Panelists also noted that the Information Sharing and Analysis Centers (ISACs) would be involved in such large-scale incidents, possibly with government support. It is unlikely a forensic investigation can be conducted on systems impacted by wiper malware since this tends to brick the system. If enough logging is in place, and has been protected in immutable storage, a forensic investigation may possibly reveal useful information. On the other hand, better detection and patching would be more applicable to a data breach or ransomware scenario, where policyholders should not only mitigate the causes of the breach, but also must conduct threat hunting to ensure there is no persistent presence of malicious actors on their networks which could lead to a follow-on attack.

In general, the panelists agreed that the scale of the incident would necessitate government involvement and industry cooperation, which would be key in determining how fast, efficiently, and easily vulnerabilities are addressed. However, there was some discussion about the extent of cooperation amongst commercial insurers, with some panelists questioning the level of cooperation that would occur without common guidelines being released.

There were also discussions about how to prioritize customers from an insurance perspective, such as a market cap or amount of insurance. Some panelists stated that the government would get involved to understand the attack at a higher level and that there would be a lot of working together across public and private organizations so that all organizations can respond rapidly. The panelists recognized the importance of government involvement and industry cooperation in responding to cyber-attacks, especially in the face of increasingly sophisticated and widespread threats. On the other hand, it is worth mentioning that there is a general distrust of sharing security incident information with the government, for fear of legal liability. In addition, many breach coaches counsel their clients not to release any written details about the incidents to reduce the risk of future lawsuits. In other words, the sharing tends to be one-sided with the government regularly sharing information with industry, but less info sharing going the other direction.

3.2.3 INFORMATION SHARING & LIABILITY CHALLENGES

The panelists discussed the challenges associated with information sharing and liability in the cybersecurity insurance industry. They found that there was a general reluctance among commercial insurers and breach coaches to share information, as they were concerned about potential lawsuits. Additionally, liability in the cybersecurity industry is not fully understood, as it is a relatively new field. The question of whether software and hardware companies should be responsible for cybersecurity liability was also raised, with the example of the automotive industry being used to illustrate the issue.

However, the panelists noted that making software companies liable for cybersecurity could lead to their folding, as the chance of vulnerability in software is much higher than in automobiles. This could result in delayed patches and exacerbate the consequences of breaches in the long run. The issue of complicated ownership was also raised, with questions of who would be responsible for liability in cases where multiple parties were involved. All these factors together made the efficacy of a new liability structure questionable.

Overall, the panelists concluded that there needs to be greater cooperation and information sharing among insurers, breach coaches, and other cybersecurity stakeholders. However, the issue of liability needs to be approached with caution, as any new liability structure could have potentially disastrous impacts on the cybersecurity industry.

Section 4: Acknowledgements

The authors' deepest gratitude goes to those without whose efforts this project could not have come to fruition: the volunteers who generously shared their wisdom, insights, advice, guidance, and arm's-length review of this study prior to publication. Any opinions expressed may not reflect their opinions nor those of their employers. Any errors belong to the authors alone.

Expert Panel Participants:

Michael Bean, Canadian Institute of Actuaries

Kenneth Crowther, Xylem

Ben Goodman, CyRisk and 4A Security and Compliance

Norman Niami, American Academy of Actuaries

Reid Putnam, Gregory & Appel Insurance

Jeremy Straub, North Dakota State University

Maochao Xu, Illinois State University

At the Society of Actuaries Research Institute:

Rob Montgomery, ASA, MAAA, FLMI, Consultant -Research Project Manager

Facilitators at the University at Albany:

Unal Tatar, PhD, Assistant Professor

Brian Nussbaum, PhD, Associate Professor

Omer F. Keskin, PhD, Assistant Professor

Doug Clifford, Program Manager of CART

Elisabeth Dubois, MBA, PMP

Dominick Foti, MBA

Brianna Bace

Rian Davis

The Society of Actuaries Research Institute would like to acknowledge the generous contribution of the Casualty Actuarial Society to the funding of this research.

Appendix A: Core Scenario Read Ahead

SIMULATED CONTENT

Albany Herald Post

Data Breach Reports Grow

Updated 21 hrs ago

ALBANY – In addition to the wave of **high-profile data breaches** reported last week, a new wave of similar events has dominated the news in recent days. **Dozens of companies, across numerous industries and sectors,** have disclosed to customers or shareholders in the past two weeks that they had suffered compromises that involved the loss or potential loss of personally identifiable information (PII), including many reporting the possible loss of credit card information. A source in federal law enforcement who has interacted with staff at more than seven victim companies said last week "The strange thing is that the companies don't seem to be related – different geographies and different industries. There's no obvious pattern that we see yet."

That said, a picture may be emerging that explains some of the connections between victims. While law enforcement officials are not commenting yet, several people tied to cyber incident response firms have made comments on Twitter and Mastodon that suggest that there could be **a common software vulnerability** across many of the victim firms. Rumors in the cybersecurity industry suggest that the **widely used software DataVex, a database management tool** that is employed by many firms using "big data" and analytics, could be the common link across targeted companies. Security researcher Juan Zania tweeted Thursday, "I would not want to be a sys admin on a network that has DataVex on it this week."

Victim firms are engaged in forensic investigations; some in the early stages, while others have been ongoing for over a week at this point. How or why DataVex might be targeted is an open question, and subject of much speculation. In a long thread on the cybersecurity industry news forum DotSlash, numerous security professionals discussed possible or rumored causes of the compromises, although almost entirely under pseudonyms rather than using their real names. A leading theory of the cause is that there was some sort of **supply chain compromise**, perhaps in DataVex's development environment, but there is no clarity yet on such speculation. DataVex's lead of product sales has deferred all questions to the public relations firm Hamilton and Breitling.

DataVex is the leader of the market in database management and ubiquitously deployed by hundreds of thousands of organizations globally. If the speculations of the supply chain compromise are correct, the impact can easily become catastrophic.

SIMULATED CONTENT

TLP AMBER

Threat Intel to Securitonin Customers on Potential DataVex Related Breach Activity

The leading cybersecurity company, Securitonin, wants all of its customers to be aware of a highly increased risk of data breach related to the software **DataVex**. Many of our customers use DataVex in their environments, and at the moment there appears to be an ongoing campaign of data theft attacks, and perhaps other kinds of attacks, targeting users of this software. Details are sketchy and emerging, but in the interest of keeping you safe, we've compiled the below details from open source, corporate partner firms, and reporting from our threat team.

1. DataVex, a widely used database management tool, appears to be the origin points for dozens of compromises and data breaches across many industries *(Source: News Reporting)*
2. It appears that **at least one known organized crime group**, sometimes referred to as Static Harpsichord (SH), **has been attacking this software in the wild for months**. The earliest reported attack **may date back five months**. *(Source: Securitonin corporate partner reporting)*
3. SH appears to have used the access to victim firms in order **to steal confidential data** that includes SSNs, credit and debit card information (Personal Financial Information), as well as trade secrets or intellectual property. There is at least one suspected case in which SH appears to have searched a victim's systems for information tied to background check documentation of federal employees or contractors with security clearances. *(Source: Securitonin Threat Analysis Team)*
4. Dark web chatter has suggested that SH may have purchased this vulnerability or access on a malware-focused auction site last summer. *(Source: Securitonin Threat Analysis Team)*
5. Analysis of Securitonin clients that run DataVex on their systems suggests that **most (i.e., more than half) have artifacts or activity on their networks that suggest the presence of SH, or a potential compromise tied to this vulnerability**. *(Source: Securitonin Threat Analysis Team)*

ACTION ITEM: ***If your firm runs DataVex (and importantly, if you are concerned your partners, third parties, or subcontractors do) please reach out immediately to your Securitonin account representative, so that we may triage your mitigation and response support.***

TLP AMBER

Appendix B: Inject 1 – Information Bulletin 1

SIMULATED CONTENT

Note to Customers on Potential DataVex Related Breach Activity – UPDATE #1

At the beginning of the third week of widespread data breaches, it is now certain that it is a **software supply chain exploit** that has leveraged the software update process of DataVex. The infectious update that was released five months ago. Based on the forensics firms working on various victims' networks, the malware has been identified as a **remote access trojan (RAT)**[1]. It allows attackers to easily control the infected systems and spread into the internal network of the victim organization. Initially, only one cyber criminal group used to exfiltrate sensitive data from over 1600 companies. However, recent investigations revealed that **the RAT was sold in dark web to other interested hacker groups on Wednesday, last week**.

The sale of the RAT to several initial access brokers on a dark web forum has **seriously expanded the scope** of the threat tied to this vulnerability. There are now **numerous cybercriminal crews** using the DataVex access vector to access a wide variety of corporate and government information technology environments. This includes organizations stealing Personally Identifiable Information (PII) / Personal Financial Information (PFI) / Protected Health Information (PHI), organizations that appear to be stealing intellectual property and trade secrets, and at least two separate **ransomware** crews that are using the access as an entry point for both crypto-ransomware and threats of hack-and-dump releases of corporate information. A blog run by a prominent security researcher at a major tech platform has started a crowdsourced list of news stories about cyber incidents tied to the DataVex vulnerability, and there are **over 3,000 ongoing events** that have already been attributed to this problem or are described as likely resulting from it, with many more ongoing events that have not yet been publicly tied directly to DataVex but could be related. In India alone, one news report has suggested that more than 200 companies have been affected; and another news report suggests that in Brazil there are at least 40 victims.

Table 1 presents the estimated losses based on the currently reported incidents. However, considering the number of organizations that deployed DataVex, this number can still increase significantly.

Table 1. Organization losses by size (Adapted from "Counting the cost", 2017)

Size	% of all businesses	Extreme Loss ($ billions)
Small *(Greater than $20m, Less than $100m)*	97.9	1.3
Medium *(Greater than $100m, Less than $1bn)*	1.8	4.2
Large *(Greater than $1bn)*	0.3	32.3
All sizes	**100%**	**37.7bn 95% CI: ($22.16bn - $53.24bn)**

[1] Remote Access Trojan is a malware designed to allow an attacker remotely control a computer and install and run any additional malware as needed.

SIMULATED CONTENT

Appendix C: Inject 2 – Information Bulletin 2

SIMULATED CONTENT

Note to Customers on Potential DataVex Related Breach Activity – UPDATE #2

Details of the DataVex vulnerability, and a **proof-of-concept (POC) piece of code for exploiting it, have been leaked** onto several paste sites frequented by hackers; presumably by someone inside one of the cybercriminal organizations that has been exploiting it. This widespread availability of the attack code to public has led to an **explosion of activity** involving attackers (of varying levels of sophistication) targeting networks running Data Vex. Many companies have attempted to remove DataVex from their systems, but unfortunately, that has often happened too late. A major telecommunications firm that provides large amounts of Internet infrastructure described scanning and attack traffic that it has seen resulting from the DataVex vulnerability as "unprecedented in the modern Internet; you'd really have to go back to some of the late 1980s and early 1990s worms to see similar percentages of Internet traffic resulting from malicious attacks."

One of the most serious developments is that a someone, calling themselves Veccs online, has released a **wiper malware** called "DataVeccS" with the POC attack code built into it – which has reportedly **destroyed large amounts of data** on some networks where it has been deployed. This user-friendly "**click-and-shoot**" malware is wreaking havoc for some major companies. A major retailer of sporting goods reported having upwards of 80% of its historical customer data destroyed. Moreover, the wiper malware is also **effective against Industrial Control System networks**, **causing disruption in the operations of critical infrastructure** sectors. It is unclear what Veccs' motivation is, and whether they are a cybercriminal, a hacktivist, an organization, or a lone individual.

DataVex has announced that they will publish a **patch** today. However, it is not yet clear that how effective the patch will be to remove the RAT in infected systems and how fast the systems will be patched by organizations around the world. As can be seen in the figure on the right, even weeks after the incident has detected and patch becomes available, many systems still wait to be updated. Table 2 presents the estimated losses based on the currently reported incidents. However, considering the number of organizations that deployed DataVex, this number can still increase significantly.

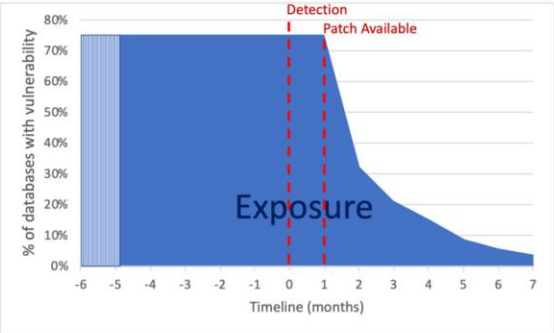


Table 2. Organization losses by size (Adapted from "Counting the cost", 2017)

Size	% of all businesses	Extreme Loss ($ billions)
Small *(Greater than $20m, Less than $100m)*	96.0	1.6
Medium *(Greater than $100m, Less than $1bn)*	3.6	8.7
Large *(Greater than $1bn)*	0.4	42.3
All sizes	**100%**	**52.6bn 95% CI: ($41.22bn - $63.98bn)**

SIMULATED CONTENT

About The Society of Actuaries Research Institute

Serving as the research arm of the Society of Actuaries (SOA), the SOA Research Institute provides objective, data-driven research bringing together tried and true practices and future-focused approaches to address societal challenges and your business needs. The Institute provides trusted knowledge, extensive experience and new technologies to help effectively identify, predict and manage risks.

Representing the thousands of actuaries who help conduct critical research, the SOA Research Institute provides clarity and solutions on risks and societal challenges. The Institute connects actuaries, academics, employers, the insurance industry, regulators, research partners, foundations and research institutions, sponsors and non-governmental organizations, building an effective network which provides support, knowledge and expertise regarding the management of risk to benefit the industry and the public.

Managed by experienced actuaries and research experts from a broad range of industries, the SOA Research Institute creates, funds, develops and distributes research to elevate actuaries as leaders in measuring and managing risk. These efforts include studies, essay collections, webcasts, research papers, survey reports, and original research on topics impacting society.

Harnessing its peer-reviewed research, leading-edge technologies, new data tools and innovative practices, the Institute seeks to understand the underlying causes of risk and the possible outcomes. The Institute develops objective research spanning a variety of topics with its strategic research programs: aging and retirement; actuarial innovation and technology; mortality and longevity; diversity, equity and inclusion; health care cost trends; and catastrophe and climate risk. The Institute has a large volume of topical research available, including an expanding collection of international and market-specific research, experience studies, models and timely research.

Society of Actuaries Research Institute
475 N. Martingale Road, Suite 600
Schaumburg, Illinois 60173
www.SOA.org