Widespread event

A single attack upon and/or failure of widely used technology could create an aggregation risk that exceeds the insurance industry's capacity to insure. In order to provide policyholders with coverage clarity and market stability, Chubb provides affirmative and specific limits, retentions, and coinsurance for such Widespread Events. Below are some hypothetical examples of widespread events.

- Global operating system cyber attack

1

1. The Event

Example Company has over 500,000 individual customers and 5,000 business clients. One day, their employees discovered that they could not access any of their workstations, critical applications or data that relied on a popular operating system. Fortunately, there were a few users in the IT team who could gain access using devices running a different operating system, with which they analysed what the issue was. An initial investigation showed critical issues within the server operating system, which had impacted multiple internal systems and customer account portals.

2

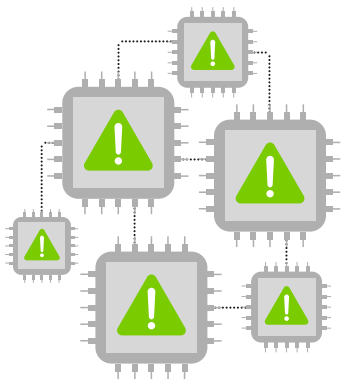
2. The Problem

Example Company reported the incident upon discovery, quickly engaging an Incident Response Manager (IRM), who triaged the incident based on the initial facts. The IRM introduced a specialist IT forensic company to assist Example Company with the investigation. The IRM also engaged lawyers and public relations specialists.

The same day, there were many media reports that businesses of all sizes and in many different industries were victims of a cyber attack, and that the issue seemed to be spreading. Multiple reports stated that all the victims seemed to be using the same server operating system. The next day, government cyber security agencies issued official statements, explaining that the attack was exploiting a zero-day vulnerability in a specific operating system, which was propagating through a commonly used, public facing, computer networking port. As software applications rely on the operating system, the functionality of applications at many businesses around the world was severely impacted, irrespective of geography, size or industry.

The incident response team further assisted with a mitigation strategy. The public relations team put together carefully crafted communications to Example Company's clients to inform them of the cause of the service disruption. Legal advisors assisted with notifying the relevant legal and regulatory bodies, and the IT specialists worked to identify possible workarounds using alternative operating systems while awaiting recovery advice from the operating system provider and security researchers.

3



3. The Solution

Over the next few days, security researchers, government cyber security agencies, and the operating system developer all released information on the attack and the vulnerability. They also provided advice for companies that had been impacted by the incident and actions for all their users to take even if they had not yet been impacted. The National Institute of Standards and Technology listed the vulnerability as a Common Vulnerability and Exposure (CVE) with a base score of 10.0 given the severe impact potential and exploitability. This is the highest score in the Common Vulnerability Scoring System (CVSS), given only to 'critical' incidents. The reports also detailed that the attack spread through an embedded tool that searched for vulnerable open ports and exploited the operating system vulnerability on all positive matches.

This was a zero-day vulnerability because it was known and exploited by hackers before the operating system developer knew about the vulnerability and created a patch. The event was widespread because the single act impacted entities and individuals outside of Example Company's limited impact group. The limited impact group may have included Example Company's individual and business customers because of the former's use of the impacted operating system and open ports. However, experts' reports highlighted that many other entities were impacted by this exploit that had no relationship with Example Company, thus excluding these parties from the limited impact group.

4

4. The Outcome

The incident response, data & system recovery costs and business interruption loss insuring clauses were all initially triggered in response to the cyber incident. Because there was information available within a few hours that showed this was a widespread event, the claim was subject to the applicable widespread event section of the policy. Loss under the insuring agreements for incident response, data & system recovery costs and business interruption was covered up to the available widespread event limits, after applying the applicable excess and coinsurance.

Widespread event

- Worldwide outage of common software solution

1

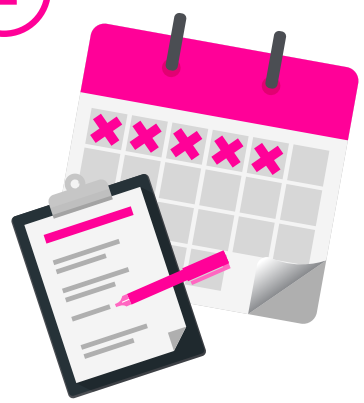
1. The Event

Example Company had locations in the UK, France, and Germany. Its production and sales locations relied on a common subscription to a cloud-based Enterprise Resource Planning (ERP) solution from a major software provider. The ERP solution enabled sales order processing, inventory management, production prioritisation, logistics management and payroll processing.

Two weeks ago, Example Company updated their ERP system from version 2.3.2 to version 3.0 after performing a penetration test and running the new version in a test environment to ensure there would not be any performance issues resulting from the update.

Last week, the ERP system crashed, restricting Example Company's access. Example Company contacted the software provider's customer support team and discovered that many customers in Europe had been impacted by the outage. Example Company also contacted the Chubb Cyber Incident Response Centre to engage an Incident Response Manager and to notify Chubb Claims of the incident. Within two hours, there was a notice on the software provider's website apologising for the issues. They advised that they were investigating a system compromise in their production environment, and to periodically check back for more information and recovery advice.

2



2. The Problem

The next day, the software provider sent an email to their customers that included a description of what to look for to check if they had been impacted by the event, and guidance on what to do next. The email stated: "If you've been operating ERP versions 2.3 or updated to version 3.0 in the last three weeks and you are experiencing accessibility issues, the problem has been caused by malicious activity in the cloud service production systems and our recovery attempts are ongoing."

The unavailability of the ERP system for Example Company lasted for five days. In the meantime, they switched to taking orders manually by phone and email, production partially continued at a significantly reduced capacity, and deliveries had to be halted as order data was inaccessible. When the system was finally available, all the historical data on orders, inventory, production status, and deliveries had been deleted and no recoverability was available. The latest notice from the software provider, which was sent by email and posted on their website, confirmed that destructive malware had corrupted customer production data as well as backup copies. The notice also detailed that the event had impacted over 30,000 ERP customers in Europe and parts of North America.

3

3. The Solution

In order to determine if the limited impact event or widespread event sections of cover applied to Example Company's policy, we needed to assess who was impacted by this event and why they were impacted. The statements made by the software provider outlined that 30,000 customers using the affected cloud ERP versions were impacted because of malicious code on the provider's production systems. The other companies had been impacted not because of their relationship with Example Company, but because of their choice of ERP system. They would have been impacted by this event even if Example Company was not a customer.

4

4. The Outcome

Information indicating that this event was affecting customers across Europe was sent to Example Company within two hours of the outage, which was the first indication that this event was widespread. Because of this, widespread event limits, excess, and coinsurance applied to the covered loss amounts. This included contingent business interruption loss, data and system recovery costs such as the cost of manual workarounds and data recovery efforts, costs for Incident Response Managers and the cost of engaging other parties to manage public relations and communications with Example Company's customers that needed to re-submit orders or manage delayed shipments.