Voluntary Shutdown: A New Normal for Cyber Business Interruption

A crippling and disabling global cyber event causing widespread disruptions became a reality earlier this year with the WannaCry and NotPetya cyber-attacks. As companies responded to the malware, several organizations determined that the most reasonable course of action to mitigate potential harm was to shut down their systems. Although this action stopped the spread of the malware, it also opened the door to an insurance coverage quandary: Are the extra expense and lost income resulting from a voluntary shutdown covered by standard cyber insurance policies?

A NEW BREED OF CYBER-ATTACK

WannaCry and NotPetya underscore the evolving nature of cyber threats. In May, WannaCry exploited a computer operating system flaw that allowed it to replicate across a network without human interaction. A month later, NotPetya took advantage of the same system vulnerability, but included several additional features that allowed it to more easily move across a network and permanently encrypt data. Both attacks caused costly and prolonged business interruptions, affecting:

- Sales and invoicing.
- Distribution and shipping.
- Communication and financial systems.

While potential losses resulting from these events are still being determined, numerous global businesses have reported significant financial harm. For example, a building materials company reported a loss of more than $250 million in first-half sales and more than $75 million in first-half operating income in the aftermath of NotPetya; a major shipping company estimated a loss of $200 million to $300 million. These losses were the result of lost revenue during prolonged system outages and extra expenses to maintain operations, including the reversion to manual processes. Additional expenditures were also needed for incident response, computer forensics, data recovery, and other remediation activities.

In some cases, however, system outages were the direct result of an entity voluntarily taking its own systems offline in an effort to mitigate harm.

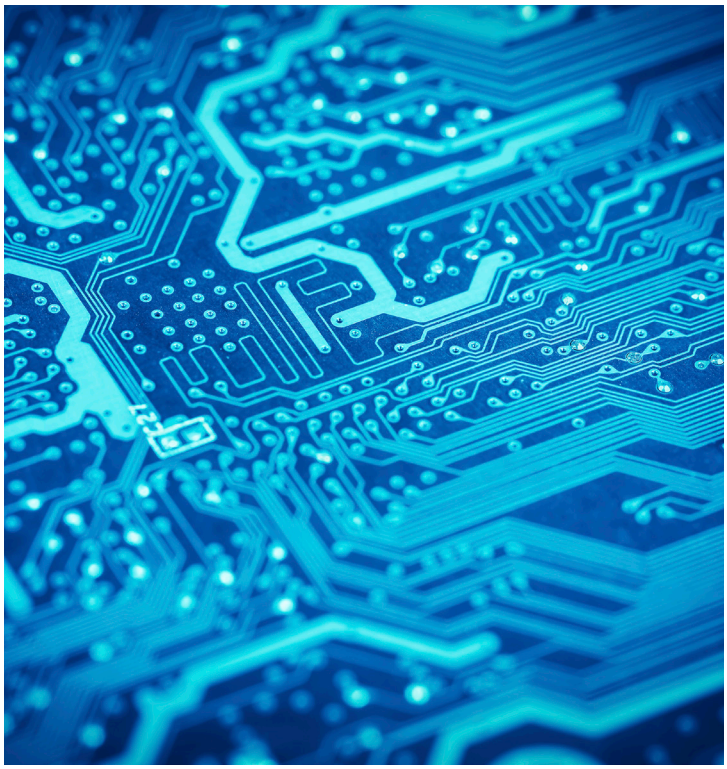
A NEW RESPONSE

WannaCry and NotPetya prompted many companies to quickly enter triage mode and seek ways to mitigate harm. Given the destructive nature of the malware and its ability to spread rapidly and indiscriminately, a number of impacted companies — upon evaluating their options — voluntarily took IT systems offline. This allowed companies to contain the malware and protect operations and data, ultimately limiting potential losses.

However, the precautionary measure also resulted in significant disruption to operations, prompting companies to look for financial recovery from their business interruption insurance policies. In doing so, insureds confronted a crucial issue surrounding today's business interruption coverage.

Cyber policies — with a few exceptions — are silent on whether the voluntary shutdown of a network triggers business interruption coverage. While there may be intent to cover this situation, many policies can be read as responding only to instances where companies have already suffered a security failure, and in some cases, system failure, leading to a network outage, rather than proactively shutting down a network as a precautionary measure to mitigate potential harm. Some policies may not intend to cover voluntary shutdowns if not specifically mentioned. Without explicit coverage, insureds may be unsure whether voluntarily taking a system offline to mitigate harm during an emergency is a viable covered option.

Traditional property policies have long encouraged insureds to take prudent measures to preserve and secure property. In many cases, they require insureds to mitigate potential losses. Cyber policies, however, have been reluctant to explicitly adopt loss mitigation concepts, though the trend appears to be slowly shifting.



SPOTLIGHT

A NEW SOLUTION

Marsh's Cyber CAT 2.0 is a streamlined insurance policy developed for organizations looking for broad cyber coverage. Cyber CAT 2.0 aims to align cyber with other available coverages, such as property. In addition to providing expanded coverage for business interruption, the policy advances contingent business interruption coverage to include non-IT supply chain suppliers, receivers, and utility/service interruption.

Cyber CAT 2.0 unequivocally addresses the voluntary and intentional shutdown of a computer system, providing best in class coverage for this growing risk. Specifically, the policy ensures a business interruption event includes:

A voluntary and intentional shutdown of a computer system by the insured in an effort to comply with an enforceable legal or regulatory requirement.

A voluntary and intentional shutdown of a computer system by the insured to limit the cyber business interruption income loss and cyber extra expenses that would otherwise be incurred.

With this added clarity, businesses can protect their systems and make timely, more informed decisions to mitigate further potential losses in emergency situations.

MARSH

WHAT'S IN YOUR POLICY?

To better understand your coverage, review your cyber policy to determine if it explicitly addresses how it would respond in the event of a voluntary shutdown. While doing so, consider the following questions:

- If voluntary shutdowns are not explicitly covered, is there language in the policy that speaks to loss mitigation or other actions taken by the insured to protect data or minimize the effects of a cyber event?
- Can voluntary shutdowns be covered by any other language in the policy?
- If the policy does not explicitly address voluntary shutdowns, how would such actions and associated business interruption losses be addressed under the policy?

If the policy does explicitly cover a voluntary shutdown, check for any conditions placed on your organization that must be satisfied either before or after the decision is made to voluntarily shutdown the computer system. Also, work with your insurance advisors to understand your coverage for claim preparation, including for technical and forensic accounting services.

For more information about cyber business interruption coverage, voluntary shutdowns, or other cyber-related issues, contact your Marsh representative or:

STEPHEN VIÑA
Senior Advisory Specialist
Marsh's Cyber Center of Excellence
+1 212 345 0399
Stephen.Vina@marsh.com

AARTI SONI, ESQ.
Senior Vice President
Marsh's Cyber Center of Excellence
+1 212 345 9768
Aarti.Soni@marsh.com