Trend
Research

Cyber Considerations for Organizations During Times of Conflict

Chief information security officers (CISOs) now face the critical roles of bolstering the organization's cybersecurity and maintaining the business's entire integrity. As geopolitical tensions rise and conflicts unfold, the cyber realm has become a battlefield where information is both a weapon and a target. These conflicts can disrupt global supply chains, trigger surges in cyberattacks, and create ripple effects that affect businesses operating inside and outside conflict zones — causing operational delays, escalating costs, eroding public trust, and increasing exposure to heightened adversarial scrutiny.

Amidst this volatility, CISOs must be proactive and adaptive. By understanding evolving threats, strengthening security measures, and figuring the human factor into the equation, CISOs can better defend their organizations against the complex risks posed by geopolitical conflicts.

What CISOs Should Know

The interconnected responsibilities of CISOs heighten the stakes. The CISO's role now extends beyond traditional cybersecurity to include managing crisis response teams, ensuring business continuity, protecting supply chains, vetting third-party vendors, securing communication channels, and coordinating with internal stakeholders, government agencies, industry peers, and international partners. Additionally, CISOs must ensure that employees are well-trained and prepared for the increased risks.

Geopolitical tensions and conflicts introduce new levels of risk. As conflicts escalate, state-sponsored cyberattacks, espionage, and the targeting of critical infrastructure become more prevalent. Economic sanctions and similar restrictions compel nations to develop offensive capabilities to bypass these constraints, retaliate against perceived adversaries, and compensate for traditional military options. A notable example is the 2017 WannaCry ransomware attack, orchestrated by North Korea's Lazarus Group, which disrupted critical infrastructure across 150 countries. Additionally, the Lazarus Group has been implicated in high-profile cybercriminal activities, including the theft of US$81 million through fraudulent SWIFT transactions.

The rules of engagement evolve during conflicts. Motivations dynamically shift during conflicts — from espionage, sabotage, and economic disruption to psychological warfare. Economic sanctions push threat actors to retaliate and escalate their activities. Financially and politically motivated cybercriminals expand their targets to exploit the resulting chaos and confusion. Hacktivist groups — sometimes used as fronts by nation-state actors like the Russia-aligned Killnet — further complicate the landscape. State-sponsored cyberattacks become more rampant to infiltrate critical infrastructure, disrupt operations, and steal data. Given the interconnected nature of today's businesses and the global systems that power

©2024 by Trentd Micro, Incorporated. All rights reserved.

them, the impact of these cybercriminal activities extends far beyond the immediate conflict zones. Moreover, attacks such as web defacements as well as malware and disinformation campaigns that have targeted Ukraine since 2014, along with cyberattacks on critical infrastructure attributed to Volt Typhoon, underscore the need for CISOs to anticipate these changes in threat actor behavior.

Humans are the CISO's unpredictable Achilles' heel. The human element remains one of the most significant vulnerabilities in cybersecurity, but it is also crucial in ensuring the organization's resilience, reliability, and readiness. Geopolitical conflicts and cyberattacks exacerbate stress and confusion, increasing the likelihood of human errors. This susceptibility is amplified by disinformation campaigns and social engineering attacks, which exploit the turmoil to manipulate employees into disclosing sensitive information or making critical mistakes. CISOs must factor humans into the equation when implementing programs that enhance workforce awareness, build strong support systems, and establish clear communication protocols.

What CISOs Must Act On

Proactive measures in advance of conflict:

Assess if the organization is a target of interest. Utilize threat intelligence platforms and frameworks to identify potential tactics and techniques that might be employed against the company.

Map out business-critical assets and services and identify their vulnerabilities. Defense-in-depth, zero-trust, and virtual patching strategies could add a layer of protection to these assets.

Diversify the supply chain to reduce risks and reinforce resilience. Build partnerships locally and internationally, especially in regions of strategic importance. Review long-term supplier contracts to identify those that could be significantly affected by disruptions and establish contingencies to maintain continuity.

Create crisis management teams. Clearly delineate roles and responsibilities as well as define operational and procedural guidelines. This preparation enables a swift and coordinated response during a conflict.

Conduct regular training for employees. Empower the workforce through regular training and simulations to prepare them for scenarios such as cyberattacks, supply chain disruptions, and security breaches.

©2024 by Trentd Micro, Incorporated. All rights reserved.

Strategic preparations and adjustments for impending conflict:

Reinforce cybersecurity defenses. Prepare to counter the anticipated increase in cyberespionage and disinformation. Ensure that all contingency plans are up-to-date. Consider if your organization should have a more diverse array of tools and defenses to prevent excessive reliance on a single vendor.

Simulate disruptions. Test for scenarios where hardware, software, or services from major suppliers become unavailable. Prepare to switch to alternative suppliers at a moment's notice to maintain operational continuity.

Prepare for increased hacktivist activities. Reinforce the integrity of infrastructure and processes. Intensify efforts to detect adversaries, as the cost of overlooking threats during conflict can be significantly higher.

Updating infrastructure and processes. Review and update the status of infrastructure, assets, and processes. Assess which systems should be fully isolated and determine where updates or changes should be temporarily disabled.

Create backups. They should be in alternative, distributed, or offline locations to ensure data resilience during disruptions.

Increase power and internet redundancy. Consider implementing autonomous power sources capable of sustaining operations for a duration appropriate to operational needs.

Safeguard critical assets. Secure and isolate critical assets to protect them from immediate threats.

Activate crisis management teams when conflict appears unavoidable. Manage the situation as it unfolds, ensuring that all roles and responsibilities are clear and actionable.

Implement communication protocols. Ensure that timely and accurate information are disseminated both internally and externally.

©2024 by Trentd Micro, Incorporated. All rights reserved.

Urgent measures when conflict erupts:

Execute emergency plans. Continuously monitor the evolving situation and immediately implement emergency response, including shifting operation models or work setups.

Ensure the health and safety of all employees: Prioritize the well-being of employees, especially those in affected areas. Ensure that safety protocols are in place and that employees are informed and supported.

Maintain constant communication with stakeholders. Keep open lines of communication with employees, partners, and customers. Ensure that accurate information is delivered on time.

Assess the trustworthiness of assets. Evaluate which assets remain trusted and which might be compromised or untrusted. Disable or erase any assets that pose a significant risk of being exploited by adversaries, whether over networks or in person.

Sustained strategies for ongoing and future conflicts:

As the initial phase of conflict stabilizes, organizations need to assess the effectiveness of the actions taken and make necessary adjustments:

Continuously monitor the situation. Adapt ways of working and supply chain activities based on real-time threat intelligence. Reassess risks and business strategies as well as reevaluate digital infrastructures.

Adapt to regulatory and policy changes that could affect operations or security posture. Trade restrictions, sanctions, cross-border controls, expropriation of assets, and law-mandated data localization could have a significant impact on business operations, supply chain activities, and compliance efforts.

Long-term planning includes on drawing specific lessons from ongoing conflicts and past crises:

Future-proof the security of digital assets and infrastructure. Enhance threat detection systems, tighten access controls, and improve measures in network segmentation and recovery capabilities. Consider diversifying energy sources to ensure business continuity. Regularly test and update these systems to adapt to evolving threats.

©2024 by Trentd Micro, Incorporated. All rights reserved.

Foster a culture of continuous improvement. Regularly revisit and update security protocols and cybersecurity practices, including incident response plans, employee training programs, access management policies, patch management, third-party risk assessments, data encryption standards, and backup and disaster recovery procedures.

Fortify strategic alliances both locally and globally. Actively participate in intelligence-sharing networks, platforms, and communities that bridge the public and private sectors. Engage with local industry groups, national cybersecurity agencies, and global cybersecurity organizations to stay informed about the latest emerging threats and best practices. Consider joining cybersecurity exercises and simulations to enhance coordination and response capabilities.

To learn more about why CISOs need to implement necessary adjustments and strategies amid conflict situations, visit https://research.trendmicro.com/ciso-guide-conflicts.

©2024 by Trentd Micro, Incorporated. All rights reserved.