MANAGING THROUGH CRISIS

Authored By:
Drew Spaniel, Lead Researcher, ICIT

Contributors:
Louis Dorsey, Sr. Director for Civilian Market Intelligence, DLT Solutions
Francisco Salguero, CIO, Federal Communications Commission (FCC)
James Saunders, CISO, Small Business Administration (SBA)
Renee Wynn, Former CIO, NASA
Jacob Olcott, VP, Government Affairs & Communications, BitSight

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

DLT
A TECH DATA COMPANY

Crises and disasters are unavoidable; especially, from the perspective of information security professionals, whose adage is to "assume you've already been hacked." It would be naïve to assume that any network was impervious to adversarial campaigns. The difference between a cybersecurity novice and a leader isn't whether they can infallibly prevent incidents; rather, the distinction lies in how they respond to crises, mitigate impacts, remediate compromises, and incorporate lessons into their risk assessment, policies, and response plans. Over 36 billion records were exposed in the first half of 2020 due to data breaches, and 68% of business leaders feel their cybersecurity risks are increasing. But not every security incident is the result of sophisticated or resourced adversaries. An estimated 95% of security incidents result from human error, and those mistakes are more likely to occur when the routine and practiced work-life of staff are disrupted by crises. For instance, when companies transitioned to telework in Q1 2020, the number of breach attempts increased by an estimated 273%, and the number of cybersecurity complaints reported to the FBI's Internet Crime Complaint Center (IC3) increased from 1000 per day to 3000 – 4000 per day.

In the long-term, organizations and their leadership are not defined by the crises that they face; instead, they are remembered for how they shouldered the burden of their responsibility, made decisions during the incident response period, triaged their systems, learned lessons, and implemented measures to mitigate impacts and future threats. During the COVID crisis and the mass migration to telework, CIO's and CISO's were on the front lines, protecting agencies from cyber threats and ensuring the continuity of essential business units and support infrastructure. In addition to technology and strategy leaders, they became crisis managers.

At the ICIT Fall 2020 briefing, Louis Dorsey, Senior Director for Civilian Market Strategy Intelligence, DLT Solutions, a Tech Data Company, moderated a panel of current and former agency C-level executives and got their perspectives on crisis management and the lessons that they learned in their experiences. Mr. Dorsey explained, "We are in the midst of a crisis that has changed and disrupted not only our personal lives, also our work. And that has been the case across all industries, from fortune 500 companies to small boutique 'mom and pop shops,' from the finance market to right here in the public sector market. I mean, almost overnight, employees had to change how they work and how they communicate with each other. The impact of technology has been more critical now than ever on our overall wellbeing and productivity." The experts on the panel opined that the organizations able to survive crises were able to trust staff to follow crisis training, adapt to evolutions in the threat landscape, and learn from the events.

Prepare and Trust Staff to Respond to Crises

James Saunders, CISO, Small Business Administration, posited that staff is the essential resource in times of crisis. He explained, "I think we were successful throughout the COVID-19 crisis. Starting back in March [2020], there was a lot going on at the time, and there are about 30 million small businesses in the US. The SBA had to get nearly $400 billion in relief out the door. There was no time to micromanage. There was no time to really sit there and review other people's work. We had to trust the team, make sure they were safe, give them the tools they needed to execute and get the heck out the way." Renee Wynn, Former CIO, NASA, concurred and added that those who were able to adapt to the challenges presented by the nation-wide shutdown were those who had practiced and prepared for similar

Copyright © 2021 Institute for Critical Infrastructure Technology (ICIT)

scenarios. She stated, "The pandemic probably isn't the place where you did your preparedness, but practicing disaster recovery, hitting the network hard, and practicing to make sure that your cybersecurity, your SOC has its visibility; Those are things you should be doing on a regular basis." Preemptively drilling scenarios and gamifying crises diminishes the shock and uncertainty around an incident and empowers staff to operate at optimally.

Adapt and Evolve to Emerging Conditions

Francisco Salguero, CIO, FCC, stressed that in addition to preparing for scenarios, we also need to prepare for changes in the environment and culture. He explained that many drills are IT-focused but do not account for sudden essential changes in environment, mentality, or behavior. The COVID-19 pandemic necessitated all three when personnel abruptly transitioned to telework. Suddenly, in addition to technical controls, staff needed to consider privacy controls, home internet activities, household management, and other factors that could otherwise disrupt their daily responsibilities.

In addition to cultural and behavioral shifts, organizations also may need to evolve their mission and programs in times of crisis. Jacob Olcott, VP, Government Affairs and Communications, BitSight, stated that this shouldn't be an obstacle for effective leaders since "Security is really a focus on business enablement." The pandemic demonstrated that rather than remaining spend-adverse, organizations should invest in solutions to enable long-term survival.

Take Every Chance to Learn

With the onset of telework, organizations had to reevaluate workflows, processes, and solutions quickly. Organizations needed to understand their deficiencies, strategically evaluate potential solutions, and determine how best to detect and defend against threats.

The staff did not have access to the same systems and technologies at home as they did in their native work environments. Leaders had to learn and commit to the most secure and efficient solutions. Remote access, VPNs, video conferencing, and other solutions became essential, and the staff was locked in a race to determine which applications and features best enabled them to complete their work securely. The strengths and weaknesses of vendor applications needed rapid evaluation. Communication and trust between staff and decision-makers were pivotal in determining which solutions were best for the organization.

Turmoil often presents opportunities for adversaries to compromise the network. To remain secure, the information security team also had to learn to recognize and thwart anomalous behaviors. Zero trust strategies proved invaluable. Especially with staff connecting from hundreds or thousands of remote access points, every action needed authenticationt, authorization, monitoringand logging.

Copyright © 2021 Institute for Critical Infrastructure Technology (ICIT)

Conclusion

The COVID-19 pandemic impacted every organization differently, but overall, those best able recover in the short-term and most likely to thrive in the long-term were had already prepared staff to respond to crises. Rather than suffering inaction and confusion, trusted and trained staff worked with leadership to shift culture and practices using lessons learned in real-time.

Copyright © 2021 Institute for Critical Infrastructure Technology (ICIT)