Enhancing Cyber Event Recovery: From Chaos to Control

Highlights from a Private Government Roundtable, hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Cohesity, July 2023

In today's dynamic digital landscape, organizations face constant cyber threats with the potential to severely disrupt operations and compromise sensitive data. Whether agencies take a proactive or reactive approach to cyber events influences the severity of the impact to the organization. Effective cyber event response and recovery mechanisms are essential for maintaining business or operational resilience.

In a recent roundtable discussion hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Cohesity, a panel of Federal experts shared insights, strategies, and lessons for improving response functions and bolstering operational resilience before, during, and after a cyber event.

Constant Learning Loop

"It's not a matter of if, but when."

Agencies are continually evaluating processes and procedures related to cyber attack resilience planning. Visibility is a key component of improving response functions, but agencies are often challenged by data availability, shared dashboards, and limited resources. Smaller agencies and subsidiaries may share dashboards with a larger organization, and may not receive threat intelligence relevant to them.

In addition to working with large industry partners, some agencies are also working with small businesses to develop resilience strategies. Large companies have resources, whereas small businesses may only have one or two individuals running IT. It's important for small agencies and small businesses to know where to access threat information and who to call when an incident is beyond their scope of control.

Due to certain agency missions, some operate with more advanced technology. As such, they are able to work directly with vendors on system updates on a yearly basis. Even so, continuity of operations remains a high priority. All agencies, regardless of technology capabilities, should have a playbook outlining the roles, responsibilities, procedures, and processes if a cyber attack were to occur. Not only should this playbook remain updated as new technology and threats emerge, but agencies should also test and practice the playbook on a regular basis.

As one participant noted, better resilience starts with awareness. Awareness of the roles and responsibilities of every employee and external stakeholders who may be impacted by a cyber attack, and the potential disruptions to business operations if a breach were to occur.

A strong business continuity plan takes into consideration the operational context of a cyber attack. Where one agency's focus may be on data security and recovery, another may need to prioritize continuity of service. Incident recovery plans should also take into account the resources available to an agency, including the level of maturity of technology and the skill level of employees.

Participants agree a key component of successful planning and recovery is strong communication among all stakeholders and the full involvement of leadership. As turnover remains high within the public sector, workforce development and continual training is of paramount importance to ensure resilience plans remain updated and effective.

Identifying and Responding to Cyber Incidents

Besides having a response and recovery plan in place, roundtable participants noted that agencies should also know what to do when the plan fails. Plans may fail if they are not continuously updated as technologies are updated. They can also fail if agencies do not test and practice them to identify areas for improvement.

Participants suggest agencies should be aware of exiting personnel and their role in the agency's continuity plan. Backfilling the position may require workforce development and skills training. It's important for agencies to remain up-to-date on the latest threats, and inform the workforce of these threats on a regular basis. Similarly, agencies should understand whether newly identified threats can be mitigated internally, or if they should defer to an outside entity.

Some agencies assign a role and responsibility to every individual in the organization, and even to external stakeholders, including law enforcement and vendors. This ensures continuity of operations and that every aspect of a cyber attack is mitigated. Agencies should also work closely with privacy vendors to quickly locate sensitive data and notify customers who may be impacted.

However, many agencies face challenges with identifying and responding to cyber attacks effectively. When agencies have many dependencies, it's challenging to identify where a flaw was located and which entity is responsible. Often, agencies don't have good visibility into the entire system, which makes it difficult to write effective recovery plans.

Agencies should have visibility of their perimeter, points of connection, IoT connections, data pathways, and locations of all servers. With so many vendors, contractors, subcontractors, and third-party vendors, agencies must be aware of the potential risks and how they intersect. Knowing how and where data is flowing helps with identifying weak links.

"If you don't understand the threat, then... recovery and response operations... may not necessarily be completely grounded in reality."

Another challenge is educating new leadership, especially if they come from a larger organization with the assumption that most tasks can be automated. Smaller agencies with fewer resources may not be able to fully execute the guidelines and directions offered by CISA or the GSA, creating frustration among leadership and staff alike.

> **“It's a little frustrating that in this day and age we still have to remind everyone you've got to start with learning how to roll over, and then crawl, and then walk, and then you practice it at each one of those phases.”**

One roundtable participant offered three pillars to help agencies make informed decisions: methodology, process, and tools. Along with ensuring the right people are at the table and the plan takes into consideration organizational context, having the right tools to quickly identify and isolate attacks are critical to effective response and recovery.

Correct and relevant tools help the agency identify what’s been exposed or compromised, which allows leaders to make informed decisions on next steps and what parts of the plan to implement. The right tool should be aligned with an agency’s recovery plan and incident response plan.

> **“Shutting everything down can't be an option”**

One of the more insidious issues facing government agencies is the lack of available and continual funding for cybersecurity tools and capabilities. As one roundtable participant noted, even the latest and greatest technology is only as secure as the back-end cybersecurity. If the backend is outdated, the risk of cybersecurity attacks increases.

In 2022 and 2023 alone, instances of cyber attacks across the public sector have increased by 125%, costing taxpayers billions of dollars. This increase is likely caused, in part, by outdated cybersecurity capabilities. One participant urged agencies to develop a better value proposition for the return on investment of backend cybersecurity technology. Unfortunately, it’s hard to have foresight on these types of investments until a scenario plays out.

Recently, the requirements for TMF (Technology Modernization Fund) dollars have changed to expand how efficiency is measured. Agencies can now measure efficiency gains as a greater impact to user experience, a more secure experience for citizens, or securing data. These changes may make funding for new technology more accessible to some agencies.

Containment and Damage Control

In order to ensure efficient containment of a cyber event, agencies should first know what is in their environment to begin with. This includes understanding what aspects of operations can be turned off and what cannot. Similarly, agencies should have a documented communication structure in order to turn off systems quickly.

As one participant noted, agencies cannot count on systems and business operations being available during a cyber event. Agencies should understand what business operations could be affected, as it could impact response operations and communications. A critical aspect of this is identity and access management. Being able to assess logs and specific account information is crucial. General network hygiene of identity and access management pay dividends in these scenarios.

Final Thoughts

- Education and training is a crucial component of prevention. Human error exists and vulnerable humans are primary targets for adversaries, which is why maintaining a skilled workforce is paramount to robust cybersecurity.
- Agencies cannot do much without a proper budget allocation. There must be funding available to develop plans, practice those plans, and hire skilled personnel to carry out response and recovery operations.
- Agencies should examine what should be included in contracts to help with disaster and recovery of cyber events. Unfortunately, not knowing what to ask can sometimes prevent the inclusion of helpful contract provisions.
- When agencies assign specific roles to personnel, they should make sure they have the authority to execute those tasks in the event of an emergency. Agencies should empower their employees to make decisions without fear of recourse.
- After real events, partial events, or testing events, agencies should examine the lessons learned and incorporate them into the response plan. Otherwise, they're just checking a box.
- From a technical perspective, agencies should look at integrations, ensuring security infrastructure has the ability to see operational infrastructure. Visibility is crucial, because if the security system cannot see it, then it cannot protect it.
- The role of leadership in plan development, testing, execution, and recovery cannot be understated. Without strong leadership support, agencies are at a severe disadvantage.