Colorado Information Analysis Center Information Bulletin

Planning Considerations for Cyber Incident Response

Planning Considerations for Cyber Incident Response

Reliable access to valid data is essential to the execution of mission essential or critical business functions. Ready access to data often means broad connectivity through multiple devices, presenting an inherent vulnerability: a large expanding attack surface. Though efficient, the breadth of this connectivity increases risk to an organization. According to the U.S. Securities and Exchange Commission 50 percent of small and midsize businesses hit with a successful cyberattack go out of business within six months.[1]

CEO's, Chiefs, Directors, and other organizational leadership, must consider the risks that come with dependency, vulnerabilities, and associated threats when planning for continuity and cyber incident response. Risk management is directly related to cyber incident response. The following paper addresses the decision makers' risk considerations when planning for an adverse cyber event.

In simple terms, Risk is the product of (Threat x Vulnerabilities x Consequence.) This paper describes types of threats, vulnerabilities, and consequences that organizations might consider when planning for a cyber incident response.

Executive Summary

Natural hazards commonly cause cascading events that may disrupt access to data. Risks from natural hazards call for integrated contingency plans that should include an IT component. Many local jurisdiction's emergency management offices routinely document the natural hazards most likely to impact their area of responsibility.

Man-made cyber threats range from simple configuration mistakes to advanced persistent threats (APT) posed by sophisticated cybercriminals or nation state actors. Associating the type of incident with potential capability of the attackers can inform mitigation spending decisions. Understanding the risk posed by an insider threat before the attack may allow cyber risk management policies to prevent a disastrous incident.

Many cybersecurity programs manage vulnerability through patching, configuration management, or robust service level agreements with third party vendors. Some programs supplement these with policies and procedures that try to minimize additional risk such as only allowing vetted applications on mobile devices. Policies that block employee access to questionable web sites may reduce the organizational risk to watering hole style attacks. Prioritizing critical IT infrastructure dependencies and testing under peak load can reveal additional weaknesses.

Business and mission consequences have visible components during incident response, but portions of those components may only be seen by an individual business unit or function. If IT staff respond to a ransomware attack by taking down an infected server(s)–they may not fully understand the negative impact to other organizational missions. The decision to not pay a ransom demand could incur costs well beyond the demand. IT staff and management are

[1] https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html

not likely the company experts at regulations, insurance or crafting messages to stakeholders, and therefore a coordinated, multi-organizational response is required.

Organizational Cyber Threat Considerations

Natural Threats

Natural hazards are a consideration for cyber incident planning, as natural events commonly cause cascading events that disrupt access to data. While it may be challenging to determine the physical location of critical IT infrastructure, it needs to be identified along with the supporting infrastructure such as power supply, back-up power, uninterruptible power supply (UPS), communication fiber, cell towers, servers, and datacenters. Take an accounting of infrastructure redundancies and single points of failure, then consider how they could be affected by natural hazards. For example, sudden interruption due to power loss or flooded IT infrastructure would likely initiate a cyber incident response. Proper response measures should include a mechanism for estimating the probable duration of outage and develop a contingency plan for affected IT networks, systems, or devices.

IT planning staff and organizational leadership both play a role in developing integrated contingency plans. Risk from natural hazards call for integrated contingency plans that include an IT component. For example, during the Waldo Canyon ire in 2012 hundreds of businesses evacuated[2] and the Hewlett-Packard office and data center was among the businesses evacuated. Hurricane Sandy, also in 2012, caused extensive flooding which complicated countless IT contingency plans.[3] Many jurisdictions already have an emergency management function that considers various types of natural hazards that are most likely to impact their communities. Through partnership with emergency management an informed IT can better communicate current risk information to an organization's contingency planners or risk managers for improved response planning.

Man-Made Threats

Cyber event trends can be applied to understand organizational risk, so that the scope and effectiveness of a cyber-incident response plan is adjusted based on threat actors' intentions and capabilities. Through information sharing and threat awareness, IT staff can develop a more accurate cyber threat picture to integrate into an organization's cyber incident response plan. For example, preparing for a threat actor demonstrating limited capability is less likely to require extensive forensics and mitigation resources, while advanced capability intrusion could require considerable investment. Preparing for website defacement is different than preparing for a ransomware attack that caused a seven hour business interruption, or a sophisticated cyber breach resulting in the sale of customer data. Potential resources include: the SANS white paper discussing how organizations can create a threat profile to assist in risk management and incident response;[4] and Sandia National Labs report SAND2012-2047 Cyber Threat Matrix from 2012 that discusses creation and implementation of a threat matrix.[5]

[2] http://www.denverpost.com/2012/06/28/colorado-springs-businesses-hit-hard-by-waldo-canyon-fire/
[3] http://www.reuters.com/article/us-storm-sandy-contingency-plans-idUSBRE8A205S20121103
[4] https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492
[5] http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-065.pdf

Nation State

Nation State threat actors have significant capability and have demonstrated the ability to bypass well implemented security, remain persistent, and hidden. Their intentions are often aligned with an adversary's military and political goals. Nation state actors have demonstrated advanced spear phishing and malware capability and impacts can range from reconnaissance to destruction of complex infrastructure.[6] Additionally, the theft of intellectual property has been a notable impact to the United States.[7] Most recently, adversaries have been accused of attempting to influence the U.S. electoral process.[8] These advanced persistent threats (APTs) could require specialized contractor expertise as part of the incident response.

Nation state actors demonstrate varied skill level and have widely varied intentions. For example, nation state actors have been credited with targeting private businesses that publicly criticize regimes: North Korea was blamed for substantial data theft and destruction of equipment in retaliation for a U.S. produced film,[9] while Iran was accused of attacking Las Vegas casinos because the owner publicly suggested the U.S. drop a nuclear device on the country.[10]

Cybercriminal

Cybercriminals range in skill level, but have consistent motivation. Their collective goal is to reap financial gain through cyber means. Cybercriminals trade in stolen data and tools and share lucrative tactics, techniques and procedures (TTPs). Cybercriminal groups may also engage in criminal activity that is aligned with nation state goals as potential proxies. Their broad scope of TTPs requires specific defense-in-depth strategies to mitigate damage. Unfortunately, a notification of a criminal cyber breach usually comes from an outside source. An informed and prepared organization is best positioned to take action to remediate the damage.

Cyber Hacktivists

Hacktivists routinely attack entities that stand in opposition to their ideology. Hacktivists commonly interrupt external facing internet based services through denial of service type attacks. This threat group generally has limited technical capability and tends to collect open source information to support their cause. This threat actor activity is often associated with high profile social incidents such as perceived police brutality.[11]

Insider Threats

This group represents a significant risk to organizations. This group has insider access and knowledge that does not require illicit skill to cause extensive damage. Not all activity in this threat group is illicit or

[6] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[7] http://www.csoonline.com/article/2973542/security-industry/chinese-spies-target-us-intellectual-property.html
[8] http://www.cnn.com/2016/05/18/politics/presidential-campaigns-cyber-attack/
[9] https://www.wired.com/2014/12/sony-hack-what-we-know/
[10] http://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/
[11] https://www.washingtonpost.com/news/morning-mix/wp/2014/08/13/amid-ferguson-protests-anonymous-hacktivists-wage-cyberwar/

intentional. IT and other staff can inadvertently cause significant impact to operations with a simple mistake or act of carelessness.[12]

Technological Threats

Consider assessing technological threats to critical information technology assets. Technological threats are accidents or failures of systems or structures, often associated with hazardous materials incidents and mechanical failures.[13] For example, chlorine gas is toxic and corrosive and if a data center were exposed; IT staff would have to implement a course of action to protect the equipment and the people.[14] A COOP plan should address identified technological threats. For example, a chlorine gas release from a railcar at a chemical plant forced hundreds of citizens to evacuate their homes and nearby industrial plants' employees to shelter in place.[15] A business impact analysis will explore exposure to technological threats and support the planning efforts to sustain access to information technology.

Cyber Vulnerabilities Considerations

The specific vulnerabilities in any given network can be impacted by factors such as design, implementation, management, policies and procedures. Networks dependencies should also be considered when examining vulnerabilities. Advance planning for a cyber incident related to a known vulnerabilities will increase efficiency and effectiveness of the response. For example, an entity could develop a mitigation strategy with the ISP to mitigate a DDoS attack. Quick access to contact information can greatly reduce the response time.

Patching

Developers release updated versions of software as researchers and threat actors find weak areas in software or devices. There is no guarantee updated software won't conflict with specific implementation or the other software,[16] so it is important that a strong policy and procedure is used to address the integrated patching. For example, the August 11, 2015 patch from Windows had a significant conflict with Symantec endpoint solutions.[17] If a network can't utilize a patch, the business is vulnerable and at increased risk.

Configuration Management

Organizations deploy various types and brands of computers, printers, programmable logic controllers, etc. The manufacturers may adjust each device enough to be technically compatible but still require IT staff to ensure they can safely interact with the enterprise network. Failed configuration management

[12] http://www.infosecurity-magazine.com/news/inadvertent-data-disclosure-by-employees-poses/
[13] https://www.fema.gov/media-library-data/20130726-1549-20490-6362/technohazards.pdf
[14] http://www.cdc.gov/niosh/ershdb/emergencyresponsecard_29750024.html
[15] http://www.thenewscenter.tv/content/news/Axiall-releases-statement-Chlorine-leak-sends-two-people-to-hospital--391494151.html
[16] http://www.securityweek.com/symantec-patches-high-risk-vulnerabilities-endpoint-protection
[17] It is important that a strong policy and procedure is used to

can have devastating effects on IT enterprises.[18] Default passwords continue to fall into this category of vulnerability and result in embarrassing breaches.

Legacy Systems

Software can meet user needs for a longer time than developers intend. Developers add features, improve functionality and might completely redesign a product over time. New capabilities may not be compatible with older software or hardware. If an IT product reaches end of life, and developers do not provide updates or other support for the "legacy" product, an organization using the product is exposed to known vulnerabilities.[19] Risk management practice examines the cost of new IT products against the price of the risk associated with the compromise of a legacy product.

Third Party Risk

Enterprises routinely leverage third party vendors to support their critical business needs. These relationships may present unknown vulnerabilities. A widely publicized breach due to third party vendors was the Target breach in 2013, when the HVAC vendor was reportedly given access to conduct authorized interaction with the network. The vendor was unaware that cyber criminals were leveraging that relationship for a payday.[20] Consider examining supplier vulnerabilities by addressing cybersecurity standards and risk management practices in both product and service contracts.

Physical Vulnerabilities

Exploitation of weak physical security of IT devices is a common tactic to compromise a network. IT devices can be co-located with other utilities in unlocked and unmarked closets, can be left unattended by personnel, and access control policies can be lax. If there is malicious intent, unplugging and swapping cables can create vulnerability. Desktop terminals and open local area network connection ports can be inviting targets for malicious actors.

Though data centers are perhaps the most essential business asset, they often fall victim to leaky ceilings, flooded floors, inadequate fire suppression systems, and dust. If general maintenance is neglected, serious vulnerability is introduced. For example, if cables and ports are not marked, it can complicate recovery time. Consider addressing requirements for physical maintenance of information technology in the overall risk management strategy.

Policy and Procedures

Sound policies and procedures, when enforced, can impact network security. For example, role based / limited access can reduce risk exposure. If every employee has administrator control of their own computer, they can expose the organization to additional risk by downloading and installing a malicious program. Business email compromise is costing businesses billions of dollars.[21] Sound policies protect against this type of vulnerability. Consider the 20 Critical Security Controls to limit exposure.

[18] http://www.evolven.com/blog/2011-devastating-outages-major-brands.html
[19] http://www.csoonline.com/article/2139382/data-protection/forgotten-risks-hide-in-legacy-systems.html
[20] http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
[21] https://www.ic3.gov/media/2016/160614.aspx

Dependencies

Power, cooling, and cabling are essential for data to be sent from place to place. Utilities are routinely impacted, and these impacts are not always visible to the IT team in a timely manner. Response procedures to extended outages are often lacking. Consider prioritization of restoration contracts with utility providers. Preferred vendors can be over committed, consider multiple restoration service and in-house redundancy. Test redundancies under peak load.

Cyber Incident Consequence Considerations

IT help desks routinely take information from users when the IT infrastructure is not meeting the user expectations. An individual user issue is unlikely to get the attention of a manager. An entire business unit experiencing an issue signifies a larger problem that must be addressed urgently.

Business and Mission Consequences

Incident response deals with consequences during prioritization of response resources and during mitigation. The authority to initiate IT response, and identify cascading impacts may require broad reach across the organization. Taking a server off-line would require coordination when impacting other parts of the organization. For example, the rising ransomware trend requires agencies to consider the business loss/exposure of using backup systems against the price of paying to release the encrypted files. The Hollywood Presbyterian Hospital suffered significant operations impact while trying to remedy a large scale ransomware infection and ultimately paid the ransom.[22] Clear response procedures may also involve coordination with law enforcement.

Regulation and Compliance

Regulations and laws mandate certain response actions when a cyber incident occurs, along with internal legal procedures. Organizations that handle payment information and patient health information offer public cases. Recently a healthcare organization was fined over $5 million because patient data was stored on an unencrypted laptop that was stolen out of an employee vehicle.[23] Regulatory and legal protections should be identified in response and continuity plans. An insurance policy may specify a process and timeline for initiating response.

External Stakeholder Impacts

Payment data and personally identifying information breaches can have far reaching impacts. The Target breach and the U.S. Office of Personnel Management resulted in high costs and national security concerns.[24] The OPM breach impacted 22.1 million people and cost the government more than $133 Million in credit monitoring for the victims alone.[25] The target breach is the evolving benchmark standard for retail breaches. The cost for legal action, brand impact and remediation could

[22] http://www.digitaltrends.com/computing/hollywood-hospital-ransomware-attack/
[23] http://energy.gov/sites/prod/files/2013/05/f0/DOE_Overview_Response-Sandy-Noreaster_Final.pdf
[24] https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/
[25] http://krebsonsecurity.com/2015/09/opm-misspends-133m-on-credit-monitoring/

total close to $1 billion.[26] Significant financial consequence demands robust preparedness and incident response, monetize your cyber risk and plan according to risk appetite.

Communication Consideration

Cyber incident communication may be between response team members or with external partners and each can impact the incident response. Response teams should consider upstream, downstream and lateral information needs. Understand how to work with the right law enforcement partners if malicious activity is discovered. An incident response plan should identify who is authorized to interact with those agencies on behalf of the company. Poor incident response can negatively impact insurance policy coverage. Some policies require notification to the insurance company even when indemnification is not requested. Also, public messaging can impact brand. In the case of the Banner Health data breach, the original incident messaging indicated limited impact to payment card services in cafeterias at certain campus locations. The company later announced the possible compromise of 3.7 million heath care records.[27] Consider public messaging as part of the cyber response plan.

Best Practice Considerations

The organizational capabilities and needs prompt incident response activities. A small jurisdiction may have less resources to conduct an effective cyber incident response, while a large corporation with may have a trained team dedicated to incident response. The responsibility for managing cyber risk spans across an organization. Risk considerations should inform the approach to cyber incident response.

Resources

CIS 20 Critical Security Controls

The CIS Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop pervasive and dangerous attacks.

Multi-State Information Sharing and Analysis Center Cyber Incident Response Guide

A non-technical guide for business managers, office managers and operations managers designed for small businesses and agencies to further knowledge and awareness regarding cyber security.

NIST Special Publication 800-61 Revision 2 – Computer Security Incident Handling Guide

This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.

Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability

This document will present recommendations to help facilities that use control systems better prepare for and respond to a cyber incident regardless of the source.

[26] https://www.google.com/#q=target+data+breach+cost
[27] http://www.healthcareitnews.com/news/banner-health-nailed-huge-cyberattack-compromised-personal-data-37-million-people

Law Enforcement Cyber Incident Reporting – A Unified Message for State, Local, Tribal, and Territorial Law Enforcement

This document details different ways State, Local, Tribal, and Territorial law enforcement partners can report suspected or confirmed cyber incidents to the federal government.

NIST Framework for Improving Critical Infrastructure Cybersecurity

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes

This document addresses the following CIAC SINs: CIAC-SIN-5, CIAC-SIN-11

CIAC Customer Satisfaction Survey

Please take a moment to complete this survey and help evaluate the quality, value, and relevance of our intelligence product. Your response will help us serve you more effectively and efficiently in the future. Thank you for your cooperation and assistance. **Click here to take survey.**

For further information concerning this bulletin please contact the
Colorado Information Analysis Center at (877) 509-2422 or email cdps_ciac@state.co.us
To report suspicious activity, please visit our website at http://www.dshem.state.co.us