CompTIA Channel Standard: Cybersecurity

The CompTIA Channel Standards were created to help improve the relevance, quality and consistency of service delivery within the IT industry. They establish specific performance requirements that will guide businesses through a continual improvement process, allowing them to embrace intelligent and highly effective business practices. Those who adopt these standards may realize their benefits in a number of ways: Increased customer confidence; heightened professional pride in the delivery of IT solutions; improved efficiency for the business as well as the client; as well as an industry-wide dedication to establishing IT Solution Providers as integral to the strategic and tactical execution of their clients' business goals.

Compliance with a CompTIA Channel Standard is not an endorsement of any particular solution, but it will serve as an assurance that the delivery of those services complies with the covered practice.

Why Comply with these Standards?

CompTIA Standards expose IT businesses to the collective best practices of the IT industry, based on years of experience shared by scores of successful peers and industry professionals. IT companies should use these ideals to guide process improvement; identify areas of strength and differentiation; while encouraging adoption of these intelligent business practices with their employees and peers. Embracing the Channel Standards will not only elevates your company's performance, it elevates the entire profession by ensuring a consistently positive customer experience.

Implementing a Standard

CompTIA recommends following these steps to embrace and implement a high standard for operations within your business.

1. Become familiar with the Standard. Review and study the related documents. Take note of differences between the Standard and the company's current practices. Discuss conducting a self-assessment of business operations based on the Standard with the management team.

2. Compare the Standard to your reality. Consider the questions posed within each of the Standard's recommendations. Is there an opportunity for improvement? Is this something that could be an organizational strong point, a key differentiator, or offer a competitive advantage for your services?

3. Identify areas where changes or other actions could make meaningful improvements. Begin by selecting one or two areas to focus on. Realize that heavy lifting may be required to achieve meaningful enhancements, but be sure the required effort fits the return. Arbitrarily achieving a standard is not helpful when that achievement only creates additional work and headaches.

4. Monitor progress and manage change. New processes can be challenging for employees to embrace. Ensure they understand the purpose of the intended improvement and include them in the planning process so the end result meets their required needs.

5. Join CompTIA as a Premier Member. CompTIA boasts a large catalog of education programs, standards, certifications, research studies, networking opportunities and peer collaboration events; each designed to help you and your business become more successful.

CompTIA Channel Standard for Cybersecurity

This Standard is based on the NIST Cybersecurity Framework and interpreted to be meaningful for IT Solution Providers. The Standard and related Workbook define the intelligent business practices integral to building a sound security posture for your organization and your clients. To demonstrate adherence to the Standard, consider earning the CompTIA Security Trustmark+. The Trustmark+ program uses the same Channel Standard for Cybersecurity and includes a 3rd party assessment of your documentation, policies, and procedures to show the due diligence undertaken by the applying organization.

Though this Standard represents the input of numerous experts over countless hours of experience and meeting with IT businesses to learn about them; the outcome will be dependent on execution and a number of market-specific as well as economic factors beyond the scope of this standard.

Only with honest self-reflection can a business effectively evaluate itself against this checklist. Throughout that process, the company and its management team can embrace incremental improvements; focus on establishing and meeting the ever-increasing expectations of their clients; in addition to creating a highly professional environment for employees.

The CompTIA Channel Standard for Cybersecurity provides intelligent business practices for the five pillars of IT security and has been categorized along those lines. By reviewing the Standard and comparing to reality, a full picture of functional best practices for your business is created. These are the five pillars of IT security:

- Identify
- Protect
- Detect
- Respond
- Recover

Category 1

Identify

This section provides the functional areas that should be reviewed, recorded, and regularly updated to maintain an understanding of the policy guidance, assets, roles, partners, and risks inherent managing the business. It also addresses planning for Security and Vulnerability Management Programs and utilizing a Risk Management Framework.

Identify has been broken down into 3 sub-categories: Inventory, Roles & Interdependencies, and Governance.

INVENTORY

Hardware Management – maintain accurate inventories of information systems and devices.

Identifying and prioritizing information assets according to criticality is essential for a business to properly manage risk, so that protections can be applied commensurate with the assets importance.

Software Management – maintain accurate inventories of its approved software and applications.

Identifying and prioritizing software according to criticality is essential for a business to properly manage risk, so that protections can be applied commensurate with the assets importance.

Data flow management – manage and document data flow management.

Without documenting the data that is legitimately supposed to flow across the network (e.g., ports, protocols, and services), it is not possible to implement least functionality precautions or even know what "bad" traffic is on the network.

External Information Systems – hosted or maintained services by 3rd parties are documented.

With the growing reliance on outsourced IT services, it is critical for businesses to understand where their data / services are hosted and what security precautions are in place to protect those critical services and data.

Resource Value Categorization – assign a classification for all assets and resources.

To apply the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations, data, whether electronic or printed, must be classified. Consistent use of data classification reinforces with users the expected level of protection of data assets in accordance with required security policies.

ROLES & INTERDEPENDENCIES

IT Security Roles & Responsibilities – user roles and responsibilities are established and documented.

It is important to know how roles work together to keep a company secure. Documenting these roles and responsibilities reduces assumptions and improves security awareness.

Supply Chain Stakeholders & Interdependencies – document stakeholder relationships within the supply chain.

Hackers have found that sometimes the easiest way to get into a network is through exploiting weaknesses in the supply chain. This involves ensuring that only reputable vendors and products are allowed to be used.

Business Role – recognize the organization's role within its industry is and identify applicable risk.

Certain businesses have wide-ranging impact on other industries. Understanding that business role and managing risk appropriately is important for businesses to take seriously.

Mission, Objectives & Activities – ensure organizational awareness of critical business functions.

Without a clear understanding of mission and objectives for a business, this can have a negative, cascading effect on overall IT security preparation. This affects the ability to protect against, respond to, and recover from incidents.

Dependencies Analysis – document dependencies and functions for the delivery of critical services.

Without a clear understanding of how critical systems work and understanding dependencies, this can have a negative, cascading effect on overall IT security preparation. This affects the ability to protect against, respond to, and recover from incidents.

Resiliency Analysis – document resilience requirements to support the delivery of critical services.

Understanding the criticality of systems will help identify what the acceptable levels of downtime are and what controls can be put in place to ensure resiliency.

GOVERNANCE

IT Security Policy & Standards - formal IT Security policies, standards, and procedures exist and are made available to all applicable parties.

IT security policies and standards establish the foundation for an IT security program. This documentation serves as the basis for being able to provide evidence of due care and due diligence, which is critical for any business that is regulated or accepts payment cards (e.g., PCI DSS).

IT Security Roles & Responsibilities – coordinate and align internal and external IT Security roles.

Having a single point of contact or an assigned group/team is crucial to avoid assumptions about who is taking care of security concerns.

Regulatory & Non-Regulatory Requirements – adhere to all applicable requirements.

Monitor the legislative and industry landscape to ensure security policy is updated in consideration of changes that are pertinent or applicable to the organization. Facilitate any validation audits, assessments or reporting that is necessary to assure compliance to applicable laws, regulations, or requirements.

IT Security Program – develop a program to govern cybersecurity risks.

The more mature a company gets with its level of IT maturity, a formal program should exist to properly manage IT security-related risks.

Vulnerability Identification – identify, document, and remediate vulnerabilities as part of a Vulnerability Management Program (VMP).

From installing missing patches to scanning for vulnerabilities, it is critical for businesses to understand technical weaknesses by identifying and correcting vulnerabilities as those are found.

Threat & Vulnerability Intelligence – receive threat and vulnerability information from quality sources.

As part of the VMP, sign up for any of numerous feeds to receive the latest threat and vulnerability information. These feeds can help highlight a vulnerability so that it can be remediated, prior to a hacker being able to exploit it.

Threat Assessments – address both internal and external threats as part of the VMP.

Threat assessments evaluate systems and applications in terms of design and architecture to ensure that current and anticipated threats are mitigated within acceptable risk tolerances. This includes an analysis of in-place systems periodically or when significant change occurs as well as the analysis of the introduction of new technology systems.

Business Impact Assessment (BIA) - assess the likelihood and impact associated with inherent and residual risk as part of the VMP.

Business Impact Assessments (BIA) are instrumental in helping businesses understand risk in their IT environments. BIAs consider all available risk sources (e.g., audit results, threat and vulnerability analysis, and regulatory compliance) and allow companies to think through actions and identify courses of action, in case something negative occurs.

Risk Determination – use threats, vulnerabilities, likelihoods and impacts to determine risk as part of the VMP.

Risk needs to be evaluated / assessed to ensure that business operations are capable of delivering services efficiently and effectively within acceptable tolerances. This helps to define risk in the organization.

Risk Responses – identify and prioritize risk responses as part of the VMP.

A well-thought risk program identifies potential or likely scenarios and the organization identifies appropriate responses, should the scenario actually occur.

Risk Management Framework – implement an enterprise-wide Risk Management Framework (RMF) to manage risk to an acceptable level.

A Risk Management Framework (RMF) is essentially a plan that ties the various risk assessment components together so that risk can be managed to an acceptable level. The RMF is more management-focused, as compared to the Vulnerability Management Program (VMP) which is technically-focused and a sub-component of the RMF.

Risk Tolerance Level – determine and document risk tolerance as part of the RMF.

Management is responsible for determining an acceptable level of risk. Acceptable risk may be governed by applicable regulatory or non-regulatory requirements.

Risk Thresholds – identify and document thresholds for incident alerts as part of the RMF.

Through assessing risk-based scenarios, management is able to identify what is acceptable and what is unacceptable risk. These scenarios help identify junctions where escalation to higher management is necessary to address the level of risk involved.

Category 2

Protect

This section details the protection measures needed to demonstrate due diligence in protecting the network and data. Access, design, training, planning, and management support all play a role in effective protection from security events.

Protect has been broken down into 6 sub-categories: Access Control, Training, Data Protection, Processes & Controls, Management, and Maintenance Protections.

ACCESS CONTROL

Logical Access Control – manage credentials to ensure access is limited to authorized users/devices.

Logical access control establishes the standards for the creation, monitoring, control, and removal of accounts. This encompasses the request process for accounts that includes authorization, approval for access by data owners, and acknowledgement of the user of their responsibilities. Periodic reviews of access permissions, as well as prompt removal of access during role change or employment termination, are also part of account management.

Physical Access Control – limit physical access to assets and resources to authorized users.

Physical access control establishes the standards for managing physical access to the organization's facilities by all parties (e.g., employees, customers, guests and vendors).

Remote Access Control – limit remote network access to authorized users and devices.

Remote access control establishes the standards for managing remote access to the organization's networks by all parties (e.g., employees, partners, vendors, etc.).

Least Privilege – permissions are managed with principles of least privilege and separation of duties.

A fundamental tenet of good IT security is to limit privileges to only those users or services that need access. Access is meant to be limited to authorized users, processes acting on behalf of authorized users, or authorized devices. Role Based Access Control (RBAC) is an example of enforcing least privilege.

Network Segmentation – implement and segregate the network.

The concept of segmenting or segregating a network is a technical way to enforce the concepts of least privilege and least access, since it prevents unauthorized traffic from traversing the network, which could do harm to the company.

TRAINING

Awareness & Training – provide cybersecurity training and awareness for all users.

It is critical to effectively and constantly educate the organization on information security precautions, privacy requirements, and information related to the protecting organizational assets.

Privileged User Training – adequately prepare privileged users for their specific cybersecurity roles.

Users who have administrative/elevated privileges (e.g., system, network, industrial control system, database administrators) are not immune from IT security threats and these privileged users have unique precautions that they should be aware of so that they do not inadvertently jeopardize the security of the organization.

Service Provider Training – third-parties understand their specific cybersecurity roles.

Validating service providers are properly trained may Include contract review, as well as the development of service level agreements and requirements. Since service providers are become crucial to business operations, service providers need to understand and abide by their roles and responsibilities.

Management Training – prepare management and executives for their specific cybersecurity roles.

Educating an organization's management on IT security topics specific to their management roles and responsibilities is very important. This reduces confusion and assumptions around IT security topics, as well as controls that may or may not be in place to protect the organization.

Security Personnel Training – train and prepare for their specific cybersecurity roles & responsibilities.

To ensure that IT security personnel are kept abreast of the latest threats and countermeasures, as well as understanding the tools they use to perform their duties, it is important to ensure IT security personnel are adequately prepared.

DATA PROTECTION

Protecting Data-At-Rest

Protecting data at rest is most commonly implemented in a form encryption (e.g., whole drive or file). While it is an evolving best practice, some industries and jurisdictions require encrypting sensitive data at rest.

Protecting Data-In-Transit

Protecting data in transit takes on many forms, most commonly is using VPNs to secure remote work connections or HTTPS to secure online purchases. The intent is to implement encryption whenever possible to protect data in transit.

Removal of Assets & Data – manage the removal, transfer, and disposal of assets and resources.

Without controlling the removal of assets from an organization's facilities, it makes physical access control nearly impossible. This greatly increases the risk of a data breach due to the loss of assets that contain sensitive information.

Availability Protections – ensure adequate availability capacity is maintained.

Many businesses have mechanisms in place to protect the up-time of their Internet presence (e.g., websites, email, services, etc.) and availability protections can take the form of redundant circuits, failover hardware and Distributed Denial of Service (DDoS) prevention.

Data Leakage – protect against data leakage.

Data leakage can come in the form of a misconfiguration of a firewall or a poorly constructed website. All companies have to be aware of what potentially sensitive information is leaking from their networks and websites for hackers to pick up.

Integrity Checking – verify software, firmware, and information integrity.

Information security integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering).

Separate Environments – separate development/testing from production environment.

The security of production networks justifies a separate network for development or testing. This allows for mistakes or misconfigurations in the test/dev environments from compromising or taking down the production network.

Baseline Configuration Requirements – utilize standards based on industry best practices.

Baseline configurations establish and enforce security configuration settings for information technology products and ensures all systems are operating under configurations that have been agreed upon according to organizational risk management.

PROCESSES & CONTROLS

System Development Life Cycle (SDLC) – implement and manage a System Development Life Cycle.

The integration of information security requirements and associated security controls into the information security architecture helps to ensure that security considerations are addressed early in the system development life cycle and are directly and explicitly related to mission/business processes.

Using a roadmap and emerging technology evaluation process, a System Development Life Cycle (SDLC) allows organizations to stay abreast of the continued evolution of security solutions, processes, and technology to identify continuous, ongoing ways to deliver technology and information securely.

Configuration Change Control – implement and manage a configuration change control process.

Configuration change control establishes a set of rules and administrative guidelines to manage changes in a rational and predictable manner. In addition, it provides for the necessary documentation of any changes made so as to reduce any possible negative impact to the users. Changes include, but are not limited to implementation of new functionality, interruption of service, repair of existing functionality, and the removal of existing functionality.

Data Backup – conduct, maintain, and test in accordance with policies and standards.

Backing up data and applications is a business requirement. It enables the recovery of data and applications in the event of loss or damage (natural disasters, system disk and other systems failures, intentional or unintentional human acts, data entry errors, or systems operator errors).

Workplace Security – security controls and mechanisms are effective regardless of workplace.

Workplace security encompasses physical access to information systems, equipment, and the respective operating environments. Physical locations and support infrastructure for information systems require protections, since computing is no longer limited to traditional workstations. Mobile computing has introduced tablets, smartphones, handhelds and other computing devices designed to be portable and facilitate productivity for remote users. Traditional controls still apply in many areas, but additional considerations must be made for portable devices and the specific configuration and enforcement of controls will likely require special consideration.

Secure Disposal of Information – destroy data in a manner that prevents unauthorized disclosure.

Federal laws, such as FACTA and HIPAA, and several state laws take the disposal of sensitive information very seriously. Sensitive data that could lead to identity theft must be disposed of in a manner that makes recovery technically impossible.

Protection Effectiveness Review – appropriate parties are made aware of the effectiveness of protection mechanisms.

Key stakeholders (e.g., customers, partners, vendors, etc.) should be kept aware of the results of ongoing reviews of the IT security program's effectiveness.

MANAGEMENT

Incident Response & Business Continuity Plans – Incident Response Plans (IRP) and Business Continuity Plans (BCP) are in place and managed.

Plans for emergency response, backup operations, and post-incident occurrence recovery for information systems need to be established, maintained and effectively implemented to ensure the availability of critical information resources and continuity of operations in emergency situations.

Response & Recovery Plan Testing – IRP and BCP are tested to ensure validity.

The only way to know for certain if a recovery plan will work is to test it. This should be at least an annual validation that incident response and recovery plans work effectively and efficiently.

Human Resources Alignment – HR processes and procedures incorporate cybersecurity best practices.

Any individual occupying a position of responsibility within the organization (including third-party service providers) needs to be trustworthy and meet established security criteria for that position. HR alignment ensures that information resources are protected during and after personnel actions such as terminations and transfers.

Vulnerability Management Plan (VMP) – develop and implement a Vulnerability Management Plan.

A Vulnerability Management Program (VMP) is a way to keep on top of managing vulnerabilities. VMP is more technically-focused and is a sub-component of the overall Risk Management Framework (RMF).

MAINTENANCE PROTECTIONS

Maintenance Support – maintenance of assets and resources is performed.

Ensuring that systems are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and service disruptions is a key component to IT security. This includes configuring operation systems and software with appropriate parameters, removing default accounts/passwords, disabling unnecessary protocols/ports, and the ongoing distribution and installation of service packs.

Remote Maintenance – remote maintenance of assets and resources is performed in an approved manner that prevents unauthorized access.

In direct support to maintenance support, remote maintenance takes on unique security concerns due to the remote nature of the support. This focuses on ensuring remote parties only have access to what they need to perform maintenance and that they disconnect when the session is complete.

Audit & Log Records – create, protect, and retain logs in accordance with the policies and standards.

Without the ability to review audit logs, putting together the facts of what happened in an incident is nearly impossible. This is why having the proper logging enabled for the correct time duration is a fundamental component to IT security.

Removable Media – restrict use of removable media through administrative and technical measures.

Access to digital and non-digital information system media need to be limited to authorized users. This requires that safeguards be in place to restrict access to this media which includes both digital media (e.g., systems, diskettes, magnetic tapes, external/removable hard drives, flash drives and other portable mass storage devices, compact disks) and non-digital media (e.g., paper, microfilm).

Least Functionality Protections – secure configurations enforce the principles of least functionality.

Least functionality is a common sense requirement where the functionality of a system, service or application is limited to what is necessary. If everything runs as an administrator/root, a compromise from malware will run with those same privileges, so limiting functionality can drastically reduce the impact of malware and other unauthorized actions.

Network Communications Protections – protect network communications.

This encompasses the control, monitoring, management and protection of communications and transmissions between information systems. It establishes the requirements for protections such as link encryption, secure file transmission protocols, retention of files on source and destination systems, integrity validation, and restrictions for access at all levels (i.e. user/process, system, and network).

Category 3

Detect

This section covers the security controls to detect events that have gotten through protections. Functions such as establishing baselines and thresholds, monitoring, and recognizing what is a threat are detailed.

Detect has been broken down into 3 sub-categories: Determining an Event, Monitoring, and Planning.

DETERMINING AN EVENT

Network Traffic Baselines – establish expected data flows to identify what constitutes "anomalous" behavior.

Baselines of network traffic can help organizations identify anomalous network behavior, such as spikes in traffic, unusual protocol usage or traffic to certain network segments.

Anomaly Detection – analyze detected events to understand the targets and methods used.

Detecting anomalies is rooted in reviewing logs, either manually or through an automated process. IDS/IPS are especially helpful in identifying anomalies. Having network baselines helps rule out false positives in anomaly detection.

Event Correlation – improve detection and escalation with information from different sources.

Event correlation is rooted in reviewing logs. This may include checking firewall logs, in conjunction with server logs, to identify the actions a hacker took while attacking a network. Aggregating logs into a Security Incident Event Management (SIEM) console can greatly improve the efficiency of event correlation.

Event Impact Assessment – determine appropriate response based on the potential impact.

Once an event is identified, it is important to understand the potential impact. This is rooted in having qualified and proficient IT security personnel who know how to assess events for potential impacts.

Incident Alerting Thresholds – establish thresholds to manage incident alerting and escalation.

Management should be aware of incidents and IT security personnel should be provided thresholds for when alerts need to be escalated.

MONITORING

Network Monitoring – monitor the network to detect potential cybersecurity events.

Network monitoring encompasses the analysis of security events and alerts as detected by the array of security and log collection devices implemented throughout the network. Security monitoring and analysis includes alert configuration and generation, event correlation as well as defining and distributing periodic reports and event statistical analysis.

Physical Monitoring – monitor physical area to detect potential cybersecurity events.

Physical monitoring encompasses reviewing physical security logs, including visitor access. Inspections of facilities also can identify potential physical breaches.

Personnel Monitoring – monitor user activity to detect potential cybersecurity events.

Depending on the risk threshold of the organization, management may monitor user activity for signs of potential cybersecurity incidents.

Malicious Code Detection Mechanisms – deploy mechanisms to detect and eradicate malicious code.

The prevention, detection and cleanup of malicious software (malware) is a basic business necessity. Protection is accomplished at varying layers including at the host, at the network, or at the gateway perimeter. Protection mechanisms must be updated periodically and frequently to address evolving threats and monitored to provide manual intervention where required.

Mobile Code Detection Mechanisms – be able to detect and take corrective actions when unacceptable mobile code is detected.

Depending on the risk threshold of the organization, mobile code may want to be blocked or otherwise acted upon (e.g., blocking, quarantine, or alerting administrators). This entirely depends on how secure an organization wants to lock down its assets and network.

Service Provider Monitoring – monitor providers to ensure conformance with the organization's policies, standards, procedures, and contractual obligations.

This encompasses the due diligence applied to monitoring the performance of service providers and their level of compliance with SLAs or other agreements to the services provided.

Periodic Checks – perform checks for unauthorized personnel, network connections, devices and software.

This encompasses spot checking on various aspects of the IT security program. Checking random controls for compliance is a way to determine if actual practices are following written requirements.

Production Vulnerability Scanning – vulnerability assessment scans are performed.

Vulnerability scanning can broadly include evaluating systems vulnerabilities, patch management levels and basic configuration management. Vulnerability scans (internal and external) is a requirement in the PCI DSS, so it applies to all organizations that accept payment cards.

PLANNING

Roles & Responsibilities for Event Detection & Response – assign personnel responsible for event detection.

Specific to event detection and response, this focuses on having the proper personnel identified and trained in their assigned roles and responsibilities.

Detection Procedures – appropriate response actions are in line with an Incident Response Plan (IRP).

This encompasses the processes in place that an organization has to detect and respond to incidents.

Response Exercises – detection processes are tested to ensure that the process is valid.

It is recommended practice to conduct exercises at least annually to ensure personnel understand their roles and responsibilities. This also validates if response plans are realistic.

Cybersecurity Event Coordination – communicate event detection information among appropriate parties.

Generally considered a Cyber Incident Response Team (CIRT), when an incident does evolve and require dedicated resources it is necessary to coordinate response activities.

Detection Process Improvement – detection processes are continuously improved.

As part of any program improvement, management should always look for ways to identify areas to improve or gain efficiencies. After Action Review (AARs) from incidents are a great way to document process improvement recommendations. This may include performing a Root Cause Analysis (RCA).

Category 4

Respond

This section addresses the readiness and ability to respond to a detected event. Analyzing, limiting the impact, and execution of the Incident Response Plan are detailed.

Respond is broken into 3 sub-categories: Analysis, Communications, and Improvements.

ANALYSIS

Alert Analysis – notifications from detection systems are investigated in a timely manner.

Alert analysis is the action a person takes in an operational incident handling capability that is focused on containment, recovery, and response activities.

Impact Understanding – evaluate the potential damage and scope of an incident.

Before closing an incident, it is crucial to understand the impact and ensure that proper escalation steps were taken, in accordance with the organization's Incident Response Plan (IRP).

Forensics – incidents that have the potential for legal action or data breach reporting utilize documented & proper forensic procedures.

Certain types of incidents may necessitate having forensics performed and this requires proper forensic procedures being utilized.

Incident Classification – classify and document incidents consistent with established response plans.

As part of most Incident Response Plans (IRPs), various classifications of incidents are identified and assigned different levels of urgency. This is to ensure serious incidents are handled more urgently than non-serious incidents.

COMMUNICATIONS:

Response Roles & Responsibilities – Incident Responders are trained and ready to react when an incident occurs.

Specific to incident response operations, this focuses on having the proper personnel identified and trained in their assigned roles and responsibilities.

Incident Reporting – events are reported consistent with established criteria in line with the IRP.

Depending on the type of incident and possible legal requirements, a business may have to report an incident to a regulatory body.

Incident Information Sharing – information is shared with appropriate parties.

Depending on the type of incident and possible legal requirements, a business may need to share the specifics of the incident with key stakeholders (e.g., customers, partners or vendors).

Stakeholder Coordination – response coordination is consistent with documented plans.

Depending on the type of incident and possible legal requirements, a business may need to coordinate with key stakeholders (e.g., customers, partners or vendors).

Situational Awareness – voluntary information sharing with external stakeholders.

Organizations sometimes share information about their incidents with external stakeholders and the industry in general in an effort to raise situational awareness.

IMPROVEMENTS

Incident Response Lessons Learned – Incident Response Plan is updated based on lessons learned.

As part of any program improvement, management should always look for ways to identify areas to improve or gain efficiencies. After Action Review (AARs) from incidents are a great way to document process improvement recommendations.

Incident Response Strategy Update – update the Incident Response Strategy.

As people, processes and technologies improve and evolve, it is necessary to periodically update incident response strategies to ensure those plans are appropriate for the organization.

Contain Incidents – mechanisms are in place to contain the scope of IT security incidents.

The focus here is to ensure that mechanisms are in place to contain incidents. This may be as simple as having response plans that require infected systems to be unplugged from the network to contain incidents.

Mitigate Incidents – mechanisms are in place to mitigate the ramifications of IT security incidents.

If a critical system was unplugged to contain an incident, a mitigation plan should include how the loss of that system can be alleviated. Be sure to consider other mitigations and their impact.

New Vulnerability Response – new vulnerabilities are identified, documented, and mitigated.

The focus here is responding to new vulnerabilities. This can be as simple as ensuring patches are installed once new patches are released and is all part of the Vulnerability Management Program (VMP).

Response Plan Execution – for incidents that require response, use a documented IRP.

The focus here is to document Incident Response Plans (IRPs) to be used as reference during incidents, rather than have incidents follow ad-hoc response decisions.

Category 5

Recovery

This section details the steps to recover from an event and overcoming any negative fall-out that results. Planning, public and reputation concerns, and getting back to normal are covered.

Recovery has been broken down into 3 sub-categories: Planning, Improvements, and Communication.

PLANNING

Recovery Plan – for incidents that require recovery, documented recovery plans are used.

Recovery planning is a methodical process and should be defined and prepared for well before an incident happens.

IMPROVEMENTS

Recovery Lessons Learned – lessons learned from recovery operations are documented and incorporated into future recovery plans.

As part of any program improvement, management should always look for ways to identify areas to improve or gain efficiencies. After Action Review (AARs) from incidents are a great way to document process improvement recommendations.

Recovery Strategy Update – lessons learned from recovery operations are used to update response strategies.

As people, processes and technologies improve and evolve, it is necessary to periodically update recovery strategies to ensure those plans are appropriate for the organization.

COMMUNICATIONS

Public Affairs – mechanisms are in place to manage public affairs.

Recovery planning should include roles and responsibilities for the possibility of addressing press releases or media inquiries. Improper public affairs responses can be disastrous for organizations.

Reputation Recovery – mechanisms are in place to perform reputation recovery.

Similar to public affairs operations, recovery planning should include contingencies for business reputation recovery. This is a business necessity to reassure customers after a publicly visible IT security incident.

Recovery Activities – recovery activities are communicated to applicable stakeholders.

The focus here is that recovery activities are executed and communicated with the appropriate stakeholders, including executive, management, and cross-functional teams that may act as part of the CIRT.

Notes

Notes

CompTIA.