Yahoo Information Security

yahoo!

“We are **Paranoid.**

We protect consumer, customer and corporate data.

We use our place on the Internet to fight for our users and for the targeted, abused and vulnerable.”

Sean Zadig
CISO - Yahoo

Paranoids

Information security standards and policies

Policy

Yahoo has a comprehensively documented Information Security Policy which incorporates the entirety of the Yahoo enterprise and features risk assessment, hardened configurations, vulnerability remediation, and incident response controls.

Policy framework

A comprehensive approach to information security is essential to protect the interests of Yahoo, as well as the interests of its affiliates, subsidiaries, customers, and vendors. Cybersecurity risks are ever-present and growing in sophistication, so preparation to meet these challenges must be measured against stringent requirements. It is for that reason that Yahoo has mapped its Information Security Policy to the Cybersecurity Framework of the National Institute of Standards and Technology (NIST CSF).

Standards

The various policy domains are supported by multiple standards. These standard documents outline specific requirements, called "controls," to be met by each business unit operating under the Yahoo corporate umbrella. Ensuring that each business unit meets these mandatory controls creates a uniform approach to information security across the entire Yahoo enterprise. Security standards and controls are administered by the Yahoo Paranoids team, who serve as subject matter experts and provide a central authority for standard implementation. When each business unit implements standards in a uniform manner, the Yahoo enterprise as a whole is more secure against sophisticated cybersecurity threats.

Controls

The specific, mandatory security requirements outlined in each standard are called controls. The controls in each Yahoo standard come from a library of security requirements within an overall Yahoo "Unified Control Framework" (UCF) that is specifically formulated to both implement security best practices at a granular level, and align with the NIST categorization of security standards. Business units are expected to view the security controls of each standard as mandatory, and implement them with the guidance of Yahoo's Paranoids.

Procedures

Documented procedures are used to guide and

standardize implementation of the controls listed in each standard. Just as standards and controls must be uniformly adopted across the Yahoo enterprise, the procedures supporting them are implemented the same way across the business units. These procedures have two levels of granularity: Standard Operating Procedures (SOPs) and Runbooks.

Standard operating procedures (SOPs)

Standard operating procedures are step-by step workflows for security processes. Each workflow incorporates both generic tasks (e.g. "peer review") as well as more detailed sub-steps (e.g. "distribute to peer business sponsors via email"), along with an official process flow diagram. It is generic enough to be applied at each business unit for the same information-security oriented task. Such procedural documents are key to effective management of a security control in diverse business unit environments.

Runbooks

Runbooks are the most granular approach to procedures supporting information security standards and controls. They are position, team, or business-unit specific instructions meant to convey the greatest detail possible. Ideally, a brand-new, untrained employee could follow the steps of a runbook and accomplish its end goal.

Guidelines

Documented guidelines are aspirational best practices for information security controls and procedures. Over time, as expert Yahoo employees have engaged with this framework of security measures, they developed improvements to mandatory controls and procedures. These improvements may improve the security profile of their team, ease control adoption, or address gaps in formal protection mechanisms. Yahoo has compiled these suggestions and built "best practices" documents that are not mandatory for adherence but may help each business unit to be as secure as possible.

Paranoids review

The Paranoids act as the stewards of policy and standard documentation that is to be applied across the Yahoo enterprise, subsidiaries, and its affiliates. Each document is reviewed at least once annually for updates and changes due to new requirements. They also store the documentation and ensure it is properly applied, in coordination with business units and subject matter experts.

Compliance

A key advantage of the Yahoo enterprise policy and standards documentation approach is that documents can be brought into alignment both internally and with external regulations or expectations. While the overarching policy framework is intentionally aligned with NIST, various controls and procedures account for the treatment of particularly sensitive or regulated data and its storage or processing. For example, GDPR or HIPAA protections are embodied where appropriate, and provide proof of fully integrated compliance with these important regulatory regimes. Furthermore, contractual obligations, including PCI DSS and Standard Contractual Clauses (SCCs), can be addressed through proper documentation.

Personnel security

Personnel security

Yahoo's Personnel Security Plan aims to protect and defend the organization's infrastructure by controlling access to secure assets, and supporting a guiding security strategy.

Personnel security overview

An effective personnel security strategy is one of the cornerstones of an organization's cybersecurity posture. It dictates how exactly the organization handles employees, determines access to secure (physical and digital) assets, and ensures the responsible handling of third party vendors and contingent workers. Yahoo has a detailed personnel security plan that addresses risks across many disciplines throughout the organization and is dedicated to maintaining a safe and secure environment for all parties involved.

Protecting both physical and access security are crucial parts of Yahoo's guiding enterprise security plan. The personnel security plan is periodically reviewed by both internal security teams as well as external auditors to minimize gaps in coverage. The plan details a global background check program, specific access paradigms, the principle of least privilege, and physical and environmental security.

Personnel security measures

Yahoo's Personnel Security controls support Yahoo's guiding security strategy by ensuring the right people have appropriate levels of authorization to access the right assets.

Access control

Specific mechanisms are in place to handle access for all employees and third parties.

Any Yahoo service provider that handles sensitive data or systems are contractually bound to adhere to the same policies as full time employees. In addition, policy states that any remote support/ troubleshoot access must be strictly monitored and required approval for the specific role.

Security roles and responsibilities for contractors are outlined in Yahoo's Information Security Policy which is reviewed on an annual basis. Access follows the principles of need to know, least privilege, and role based access control (RBAC) via an automated process to limit or remove access based upon internal user roles.

The principle of least privilege states that users are limited to access rights for the bare minimum permissions they need to perform their work. Under the principle of least privilege, users are granted permission to read, write or execute only the files or resources they need to do their jobs. In other words, the least amount of privilege necessary.

Background checks

Yahoo is committed to maintaining a safe and secure environment for its employees, contingent workers, visitors, and members. Background checks help Yahoo determine employment eligibility, protect workplace security and safety, and support compliance efforts. They also assist Yahoo in protecting our property and assets. Background checks are mandatory for individuals employed or engaged by Yahoo's operations to work or to provide services as employees, interns, agents, officers, Board members or contingent workers in our physical environment, in our network, or with our information. The Policy applies to individuals at any level of the organization, and to all Yahoo business entities and wholly owned subsidiaries. Background checks comply with local laws and regulations.

Physical and environmental security

Yahoo's personnel security plan covers both physical and environmental security. Each Yahoo location is a part of the multiple safety processes and procedures that protect its employees. All Yahoo locations require badge-only access for entry. In addition, most locations have front desk reception with 24/7 security monitoring to detect a number of risks such as fire, intrusion, or any other physical and environmental emergencies.

Data Centers have a similar policy when it comes to physical security. Yahoo uses the practices outlined

in NIST SP 800-53 to support its Data Center Physical and Environmental Protection policies. Dedicated operations teams monitor the physical locations as well as the overall environmental controls on a regular basis to maintain the overall health of the Yahoo infrastructure.

Yahoo data centers use multiple layers of security, including both physical and electronic access controls. Cameras monitor the space internally to document any unauthorized or attempted unauthorized access into any datacenter physical location. In the event of an outage or unplanned event, all security mechanisms must be in place including the use of redundancy in the system for protected equipment.

Risk management

Risk management

Yahoo has a robust risk management strategy that focuses on all aspects of the Yahoo enterprise, ranging from security bugs in software to supply chain & supplier risks.

Risk management overview

Information security is paramount at Yahoo. There are inherent security risks that accompany any IT infrastructure - Yahoo is no exception. Cybersecurity risks grow year after year as attackers and threats become more and more sophisticated. All cybersecurity decisions at Yahoo are driven from a thorough understanding of the organization's assets, vulnerabilities, threats, data, and network systems. Risk management at Yahoo involves constantly refining the organization's risk tolerance strategy, formally assessing security risks both internally and via third party auditors, tracking risks using robust ticket management and threat intelligence platforms, and analyzing risks posed by third party vendors and suppliers.

Risk policy

Yahoo has a guiding risk management framework in place which defines how employees and systems should act in order to secure Yahoo and its consumers. Yahoo's formal risk management strategies and risk assessments are used to evaluate how well Yahoo's existing controls and policies protect customers and employees and shield the enterprise from risk. Many inputs impact risk decisions at Yahoo, including regulatory requirements, contractual obligations, business drivers, and threat events. Yahoo frames and classifies risks based on these inputs in order to properly manage risk in the enterprise and formally evaluate its current risk levels.

Formal risk assessments

Formal risk assessments are measures taken to evaluate the universe of risk at Yahoo. They are extensive operations that assess what potentially could go wrong, the likelihood of risk events occurring, and the impact to the firm's writ largely if the event were to happen. They also provide direction on what gaps exist in current controls and how/to what extent these should be alleviated. Yahoo follows industry standard risk assessment procedures with general guidance from NIST 800-30. The risk assessment process at Yahoo includes the following elements:

System characterization

The first step to any formal risk assessment at Yahoo is to fully characterize Yahoo's infrastructure (people, processes, and technology). To initialize any assessment, analysts on teams across Yahoo's platform and security teams collaborate to provide information regarding asset details, configurations, system diagrams, interface information, processes, personnel lists, network schemas, etc. about the items in scope in order to ensure that the risk assessment is thorough.

Risk identification

Internal or external security and risk assessment experts across teams walk through systems in order to identify potential threat vectors. For example, Yahoo's Bug Bounty program and Vulnerability Management team are dedicated to identifying technical vulnerabilities on Yahoo's infrastructure. Other teams across Yahoo's Paranoids play large roles; for example, a network security expert might note that one network segment is particularly vulnerable to a DDoS attack due to a gap in a process, or a product security expert at Yahoo might note that a group of encryption keys is vulnerable because there is no separation of duties mechanism in place. Outside of the Paranoids organization, risks also arise from M&A activity, PCI assessments, and third party security reports. All these threats are compiled into securely protected documentation with specific metrics such as number of users on the platform, value of data impacted, etc., in order to conduct impact analyses and prioritization.

Impact analysis

After threats have been identified and the systems in scope characterized, the impact analysis determines the scope of potential damage that the threat event would cause if it occurs. Some questions to consider when looking at a threat event would be:

Which information systems and processes are impacted by the threat event? How critical are they to business operations?

What are the interdependencies of these impacted systems and processes?

What is the required uptime/maximum downtime for each of these systems?

Probability calculation

The likelihood assessment stage of the risk analysis process is critical. A threat event with an extremely high impact can have relatively low risk to the organization if the likelihood of it occurring is close to zero.

Controls examination

Yahoo utilizes industry standard procedures in order to answer two key questions regarding existing mitigating controls:

Are there any gaps in current control coverage?

Are the currently in-place controls sufficient to defend against attack?

Yahoo utilizes both in-house teams and third-party experts to periodically reexamine Yahoo's suite of defensive controls. Maturity models are used to measure Yahoo's existing controls against industry standard Cybersecurity Frameworks such as NIST. Controls ranging from technical network controls (such as firewall configurations) to administrative controls (such as a remote VPN policy) are reviewed in each risk assessment.

Scoring and prioritization

The final step of the risk assessment process is the scoring and prioritization phase. Prioritization is based on a variety of risk inputs collected during the previous assessment stages, most notably exposure, impact, and likelihood. This allows for analysts to easily run reports and provide executive level visibility into security risks across Yahoo's enterprise.

Risk tracking, reporting and treatment

Yahoo takes the final outputs from each stage of risk assessments and uses them to track various risks across the enterprise. Analysts across Yahoo's many teams create reports that flow up into executive-level dashboards to provide holistic views of risk across the firm.

Security bugs

Yahoo's Security Bugs (or, SBugs) program is a robust solution for tracking and treating technical security issues across the enterprise. Yahoo has dozens of teams dedicated to hunting down SBugs across Yahoo's software platforms and meticulously tracking them. Yahoo's Risk Management team has trained analysts dedicated to conducting statistical analysis across tracked security bugs in order to inform the enterprise's strategic initiatives. These analysts create executive level reports that inform business owners and leadership about the most pressing technical risks the organization is currently facing, timelines for risk remediation, and which groups in the enterprise own the most risk. Yahoo's Paranoids work with the business owners to provide guidance on remediating the issues.

Vulnerability management

Vulnerability management

Yahoo has a dedicated team focused on ensuring that vulnerabilities in the company's infrastructure are identified, tracked, and remediated within the standards set by Yahoo's guiding Information Security Policy.

Vulnerability management overview

In information security, a vulnerability is a weakness which can be exploited by a malicious actor or adversary. Vulnerabilities arise from a multitude of causes, such as misconfigured systems, design flaws, and bugs in code. Yahoo's Paranoids have a dedicated group for handling vulnerabilities in the infrastructure - the Paranoid Vulnerability Management team. This team utilizes automated scans and internal research to detect, track, and perform remediation of vulnerabilities on Yahoo's systems. Vulnerability scans are performed regularly and are then tracked to remediation. Once a vulnerability is detected, the team assigns a ticket to the team responsible for the system with timelines for resolution. Categorization and SLAs are determined by the Paranoids Risk team.

Scanning

A key responsibility of the Paranoid Vulnerability Management team is to continuously scan systems in order to proactively identify vulnerabilities, misconfigurations, and flaws, and then ticket findings for remediation according to SLAs determined by Yahoo's guiding information security risk frameworks. Several types of vulnerability scans and assessments are employed in order to align with the enterprise's guiding Information Security Policy and SLAs.

Perimeter scanning

Yahoo conducts periodic perimeter scans across its external network infrastructure to continually assess the most exposed assets on the infrastructure for both vulnerabilities and mis-configurations.

Internal scanning

In addition to perimeter scans, Yahoo also conducts a variety of internal scans. Internal scans examine assets in the internal networks, in data centers, and public clouds for vulnerabilities and misconfigurations. They consist largely of discovery scans and unauthenticated network scans.

Agent-based scanning

Yahoo also conducts agent-based scanning. Yahoo uses an agent-based scanning regimen to give high-fidelity authenticated scan information at the host level. This will sometimes provide additional context about a potential vulnerability or misconfiguration that would not normally arise from a basic perimeter or internal unauthenticated network scan.

The results of all scans are reported directly to the Vulnerability Management team in real time.

Maintenance requirements

Yahoo policy states that IT systems and software/firmware must operate at the highest supported release which actively minimizes the number of known vulnerabilities due to system misconfigurations.

Yahoo strives to ensure that installed software/ firmware versions are updated, upgraded and patched promptly when a known vulnerability is involved.

Newly disclosed vulnerabilities

The Paranoids employ a layered approach to identifying vulnerabilities on Yahoo's infrastructure. One facet of this layered approach is Yahoo's "Newly Disclosed Vulnerability Response." Yahoo's Paranoids have a detailed playbook that walks step-by-step through the identification and response to vulnerabilities that have not yet been identified on Yahoo's infrastructure (these are called New Vulnerabilities, or zero days). The playbook gives specifics for monitoring and identification, and drives the process through to remediation and

mitigation of the newly discovered vulnerabilities. Yahoo's Newly Disclosed Vulnerability Response process is cross-disciplinary within Yahoo's Paranoids, including participants from security management, Yahoo's Incident Response team, and Yahoo's Security Bugs team. This provides the needed flexibility to the Paranoids to work together to quickly identify, analyze, triage, and understand the impacts of never-before-seen vulnerabilities.

Network administration and change control

Secure network administration

Yahoo's Network Operations organization uses state of the art tools to ensure that all enterprise systems operate seamlessly and securely.

Overview

Network security is one of the most critical stage gates in securing Yahoo's data and services. Yahoo's network is the perimeter that encircles the enterprise's valuable data and assets. Yahoo's Network Operations organization and Yahoo's Paranoids are dedicated to the enterprise's network security. They are responsible for ensuring that no violations of Yahoo's Information Security Policy and guiding strategy are deployed onto the network. These teams are staffed with engineers who work with various Yahoo business units to not only remediate any existing network incidents, but also assist in hardening system and network infrastructure. Secure network administration at Yahoo considers a wide breadth of functions such as: utilizing industry standard network hardening mechanisms, ensuring that the network is standardized, making sure that changes to the network are well-defined and approved prior to deployment, conducting rigorous network risk assessments, and managing the implementation of preventative mechanisms and controls for emergency operations.

Defending the perimeter

Yahoo's network engineers and engineers across their Paranoids teams have implemented a variety of industry standard controls in order to harden the network perimeter. Yahoo's network and system environments are logically separated in order to ensure the isolation and protection of sensitive data. This defined separation allows Yahoo to strategically place network tools such as firewalls, intrusion detection systems, and intrusion prevention systems across the infrastructure at critical choke points. Yahoo has teams of trained experts dedicated to both monitoring the configurations on network defense systems and reviewing the logs coming from them to ensure that all threats to the network are thoroughly tracked and negated. Yahoo's information security compliance teams maintain rigorous sets of policies, standards, and procedures that all network perimeter operations abide by. These policies and procedures define, for example, how administrators at Yahoo configure the vast array of firewalls on the infrastructure up to secure, effective levels.

Network standardization

Network standardization is one of the key philosophies that guides Yahoo's network security strategy. Network standardization eliminates one-off cases on systems and ensures that all Yahoo systems, including those from any of Yahoo's legacy infrastructures can cooperate seamlessly. To achieve this high level of standardization, Yahoo uses a "zero-trust" paradigm in provisioning new network devices. This means that when new network devices are added, it is assumed that untrusted or trusted actors could be attempting to use it - this is a guiding principle that leads to total standardization and rigorous authentication of access to devices. Besides minimizing network resource usage, keeping network hardware and software standardized also allows a more streamlined approach to network monitoring and defense implementation. With full standardization, communication across personnel and infrastructure becomes simpler, and network security incidents become easier to manage.

Secure change control

Change is inherent to any organization, but many do not realize that change management is, above all, a security issue. Each change to an organization's systems: the addition, removal, or modification of existing policies and systems, can introduce new risks.

Network change control

Yahoo's Network Operations organization values effective change management. Network policy

changes are carefully reviewed in order to prevent the creation of violations on Yahoo's networks. All policy changes to the network must undergo request and approval processes. The Yahoo Paranoids team has change approval oversight; the Paranoids work closely with business units to ensure that they not only adhere to the guiding information security strategy, but they understand it as well. Yahoo's Network Operations organization provides expert support to the Paranoids organization in order to validate that both the business units' and Paranoids' operations remain in compliance with network security requirements. Yahoo typically manages major network policy changes using a thorough change management request (CMR) process.

Systems change control

Yahoo Change Management policy aims to reduce risk and service disruption caused by changes across the organization. Consolidation efforts in large organizations such as Yahoo can be extremely complex and challenging.

Change Management drives the adoption of best practices and secure process improvement for the enterprise. Change Management Processes provide guidance and procedures for implementing proposed changes as well as a means to manage change approvals.

Network risk evaluations

Members outside of the Network Operations organization such as Yahoo's Vulnerability Management team (and others in Yahoo's Paranoids) provide independent assessments and evaluations to ensure the highest rigor in internal network risk analysis. Yahoo regularly runs scheduled, automated vulnerability scans against all publicly facing systems to ensure that all systems are hardened to secure levels. Yahoo does not share specific infrastructure details or vulnerability information outside of authorized personnel. The results and reporting documentation from risk and vulnerability assessments are stored securely. These internal network risk evaluations are conducted separately from annual, formal third party risk assessments that evaluate how effectively Yahoo's security mechanisms align with the enterprise strategy.

Cryptographic architecture

Yahoo's cryptographic architecture provides a framework for how to manage encryption processes within the Yahoo network environment. Encryption is one of the foundations of cybersecurity. It is the process used to protect and encode the transmission of secure data across communication channels within and across a network infrastructure. A cryptographic architecture is a wide-ranging framework. It describes the mathematical algorithms, protocols, access mechanisms, and encryption key characteristics used to successfully execute encryption on or across a network. Yahoo's team of cryptography experts have engineered a mathematically sound, proprietary cryptographic framework that protects against unauthorized access to Yahoo's most sensitive systems.

Secure software development

Software security

Secure software development at Yahoo ensures that applications are developed with security as a priority. Yahoo utilizes a secure product development methodology to help developers integrate security into the creation of applications. Yahoo's industry standard secure product development practices attempt to address security issues before they manifest in production systems. These mechanisms drive security assurance activities methodically throughout the product's lifecycle.

Yahoo developers work with in-house security experts, called the Paranoids, to review security requirements, implement architecture and design reviews, conduct code reviews, employ threat modeling, utilize web application security testing, conduct penetration testing, and practice secure by design methodologies to help bring Yahoo's projects and applications to a secure baseline. Yahoo's information security experts regularly present at conferences nationally and developers are trained in-house in the implementation of secure development methodologies.

Secure by design

Software developers on Yahoo teams implement security into their software following a "Build Security In" paradigm. Security experts within Yahoo's Paranoids engage with developers to conduct security plan reviews, requirements reviews, architecture reviews, automated and manual code reviews, and remediation validation throughout development. These mechanisms strive to ensure that the technical security controls implemented in an application support Yahoo's guiding security strategy.

Planning and requirements

Yahoo's Information Security Policy provides high level information security requirements that teams strive to integrate into project requirements and analysis activities. Developers work with security experts to leverage assurance gates at the outset of project design to help the team understand risks during periodic checkpoints. Yahoo's development teams utilize software security plans to identify and baseline integrated security activities in order to achieve the appropriate level of product development security assurance against Yahoo's business objectives. Further, the team advises on patterns and antipatterns, secure feature development, and proper security testing/ QA.

Design

Paranoids at Yahoo provide specialized expertise and guidance to developers in order to help ensure secure application design.
Development projects at Yahoo use threat modeling in order to support the deployment of layered defenses.

Implementation

Paranoids provide security training such as OWASP-based Web Application Security, Secure DevOps, Secure Development in Java, and other relevant role-based instructor-led training to developers. These trainings are periodically refreshed in order to stay abreast of the newest secure code industry standards.
Yahoo developers are trained in safe coding processes such as conducting frequent code analyses that can be integrated into developer build and deploy DevOps pipelines and only using development tools that pass Yahoo security checks.

Testing

During code development and implementation, developers use a variety of testing techniques such as dynamic analysis, fuzzing, and penetration testing to ensure applications behave properly and protect the confidentiality, integrity, and availability of data.

Release

Prior to the release of applications, Yahoo conducts final security checks, approves the release, and ensures the application complies with Yahoo's Information Security Policy.

Maintenance

Yahoo has several teams which monitor aspects of an application's security performance while it is fully operational through fully-fledged patch deployment, vulnerability management, and penetration testing mechanisms. Yahoo operates a renowned bug bounty program that leverages the external researcher community to continually identify vulnerabilities in production for subsequent remediation.

Security assurance and testing

Yahoo strives to ensure that its software remains secure to the standards set by Yahoo's guiding Information Security Policy by utilizing advanced testing and review strategies. Developers attempt to validate the results of secure design and implementation through automated and manual penetration testing, manual code reviews, and a variety of vulnerability assessments and scans. These mechanisms work towards the goal of ensuring that code is written securely, executes as intended, and complies with Yahoo's Information Security Policy. Yahoo has teams dedicated to security architecture analysis, secure code review, vulnerability scanning, vulnerability management, bug bounty, cloud security, penetration testing, and compliance auditing. Experts from these teams work together and provide their expertise to developers in order to propagate the development of secure code.

Third party software security

Yahoo has teams dedicated to conducting vendor risk assessments which, among other assessment areas, examine third party software. Automated and manual reviews are used to identify potential vulnerabilities in implemented code. Yahoo's secure product development mechanisms strive to ensure that third party and open source code implementation abides by Yahoo's Information Security Policy.

Protecting "CIA"

Yahoo's secure design practices and standards raise confidence levels that security mechanisms in Yahoo's information systems protect the confidentiality, integrity, and availability of data, or "CIA."

Confidentiality

Confidentiality is the notion that data is protected from disclosure to unauthorized third parties. Yahoo uses access controls and other secure authentication mechanisms to help ensure that the only people accessing sensitive data are those with proper, verifiable authorization.

Integrity

The integrity of information refers to its protection from unauthorized modification. Yahoo implements various cryptographic mechanisms to help provide assurance that data sent both across and from Yahoo's systems is sent as intended.

Availability

Yahoo attempts to assure that information, data, and communication that flows across Yahoo's systems is readily available when it needs to be. Yahoo uses a variety of secure network and development strategies such as load balancing, over-provisioning bandwidth, cutting-edge network monitoring, and endpoint defense to help ensure that systems are adequately protected from denial-of-service attacks.

Incident response

Incident response

Yahoo's incident response plan is an organized approach to detecting, containing, remediating, and investigating security events.

Incident response overview at Yahoo

An effective incident response strategy is one of the cornerstones of an organization's cybersecurity posture. It dictates how exactly the organization responds to security incidents such as breaches, compromises, DDoS attacks, phishing attempts, etc. Yahoo has a detailed incident response plan that sits underneath the organization's Chief Information Security Officer (CISO) and is successful through close collaboration with the organization's business units. The response plan is periodically reviewed by both internal risk assessment teams as well as external auditors to ensure that there are no gaps in coverage. The plan details a specific response process (ranging from incident detection through incident remediation and lessons learned), escalation mechanisms, communication channels and methodologies, roles and responsibilities, and many other emergency considerations.

The incident response plan

Yahoo's incident response plan documentation covers all of the major stages of incident management in depth.

Preparation

Yahoo's incident response plan specifically enumerates the preparation phase of an incident. Yahoo's Legal team works closely with the Incident Response team to create effective standards, procedures, and runbooks which explain the roles, responsibilities, and mechanisms utilized to respond to any kind of incident contemplated on Yahoo's infrastructure. Detailed communication plans are outlined and consistently refreshed with updates based on changes to enterprise technology.

Detection

The incident response plan goes into detail on the specific mechanisms that security teams at Yahoo use to detect events across the network infrastructure. Tools (both developed in-house and acquired from third parties), logging standards, declaration criteria, and severity analysis procedures are all determined. Securing digital evidence and proper chain of custody utilization is paramount here to ensure this data maintains integrity throughout the investigation.

Containment

Yahoo's incident response plan specifically details how incidents are contained once they are detected on the network. Yahoo's network infrastructure uses logical system segments and isolation mechanisms to ensure that, even if a breach occurs on one part of the network, this impact is minimized and it cannot spread to other parts of the network. Vital information systems are completely separate from the network to further minimize this risk. If one team's credentials are obtained by an unauthorized actor, Yahoo's access control mechanisms such as two-factor authentication, network segmentation, least privilege, dual control, and separation of duties all ensure that the damage is contained. Yahoo's extensive audit trails also make it easier to work on the next step in the incident response process, eradication.

Eradication

The eradication stage of an incident response plan details the mechanisms and workflows that incident response team members use to remediate incidents from the environment. A large part of the remediation is root cause analysis. Root cause analysis is conducted in order to understand both the source of the attack and the vulnerability the attack exploited. Some analysis mechanisms include network correlation strategies, log analysis, timeline analysis, and memory/string artifact analyses. Once the root cause is properly understood, network administrators work together with the incident response team to install trusted, secure patches, and then harden the network to ensure that the event cannot happen again.

Recovery

One of the key aspects of the incident response plan is the recovery stage. This stage is critical as it involves restoring systems back to pre-incident operations (while still having eradicated the root cause of the incident). This stage involves invoking business continuity & disaster recovery procedures, restoring systems from the appropriate checkpoints, validating that systems are ready to be operating in business as usual functions, and implementing Legal and PR operations (as necessary).

Continuous improvement

The final stage of the incident response plan is continuous improvement. Yahoo's Paranoids work together after incidents to formally debrief and determine lessons learned via after action reports. The team creates long-term plans for shoring up weaknesses, mitigating newly discovered vulnerabilities, and updating and improving the incident response plan.

Engaging with third parties

Yahoo may rely on support from third parties or law enforcement organizations to offer supplemental or uniquely specialized services in order to assist in containing, eradicating and recovering from an attack. Yahoo has specific documentation in its incident response plan that establishes a framework for properly and securely interacting with third parties during an investigation.

Updates and review

Yahoo's incident response plan is frequently reviewed by risk assessment professionals, internal legal professionals, and third-party independent auditors and regulators to ensure thoroughness.

The incident response team

Yahoo has several teams dedicated to securing the organization from malicious actors and activity.

Security operations center

Yahoo's Security Operations Center (the SOC) monitors and investigates security events on Yahoo systems using state of the art tools and data analysis to look for signs and signatures of potential compromises. They are the "eyes on glass" that initially protect the infrastructure and escalate the most severe security events.

Incident responders

The incident responders are the experts at Yahoo who serve as the escalation point for severe security events. They conduct forensic analysis, manage and update the incident response plan (with input from many stakeholders), and regularly conduct their own analysis of security events on the infrastructure.

Business continuity planning

Business continuity planning

Yahoo's Business Continuity Planning Team maintains responsible contingency plans for products and applications to minimize service disruption.

Overview

Yahoo has a mature Business Continuity Planning Program responsible for ensuring all critical infrastructure, applications, and services are resilient in the event of disaster. The BCP Program spans the entire organization, sits within Yahoo's Infrastructure Services and Operations Group, and has the active support of Yahoo's Leadership. The objectives of this program are to minimize disruptions to service, safeguard sensitive and confidential information, and to respond and recover rapidly in the event of disruption. Yahoo provides a multi-failure disaster recovery capability by utilizing multiple hot sites across the globe.

Yahoo monitors service continuity with upstream providers in the event of provider failure. Service providers are governed under rigid service level agreements to ensure reliability. Upstream provider service continuity is continuously monitored and logged. Yahoo uses multiple service providers in support of critical infrastructure and has mechanisms in place for rapid cutover to maintain services. Business continuity and redundancy plans are in place for all Yahoo critical functions impacting customer availability.

Yahoo's BCP plan

Yahoo complies with Contingency Planning for Information Technology Systems. Yahoo has the following mature practices, procedures, and tools in place:

1. Contingency Planning Policy Statement. The formal policy provides the authority and guidance necessary to develop an effective contingency plan
2. Checklist Requirements and Recommendation. The tier structure helps identify and prioritize critical IT systems and components
3. Multiple Preventive Controls. These are measures that reduce the effects of system disruptions and increases system availability.
4. Recovery Strategies. Thorough recovery strategies ensure that the system can be recovered quickly and effectively following a disruption
5. IT Contingency Plan. The contingency plan contains detailed guidance and procedures for restoring a damaged system
6. Planned Testing, Training and Exercising. Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness

Business continuity planning Governance

Business continuity planning procedures at Yahoo are governed by a central team. The BCP team reviews Yahoo's recovery plans and ensures their continued relevance. Yahoo and its network is architected with resiliency, redundancy and availability in mind, and is monitored for performance and problem identification. Yahoo incorporates business continuity capabilities into all delivery capabilities. Platforms are monitored using a proprietary algorithm for determining capacity, performance and security events. Yahoo also has formal processes for data ingestion and during component failover measuring the Recovery Time Objective (RTO, which is the target time set for the recovery of the IT and business activities after a disaster has struck) and Recovery Point Objective (RPO, is focused on data and Yahoo's loss tolerance in relation to the data), against the Recovery Time Actual (RTA, which is the real-time it takes to restore functionality to the property).

Environmental disaster

Yahoo's data centers are strategically placed around the world in generally low environmental risk areas. In the event that one of Yahoo's data centers is impacted by a natural disaster, Yahoo will follow standard operating procedures and BCP plans. Yahoo employs a dedicated data operations team

which monitors systems, environmental controls and overall health of the Yahoo infrastructure.

Data protection and backup

Network systems, configurations and source code are geographically redundant across multiple data centers.

Redundancy

Yahoo ensures resiliency with a presence in multiple datacenters as well as regional and continental PoP sites that utilize redundant network equipment. This in conjunction with cloud platform technology allows Yahoo to reduce production incidents and provide a more robust user experience.

Monitoring

Yahoo performs end-to-end health checks for system performance and availability using proprietary tools as well as third-party monitoring solutions. Yahoo also monitors the health of its sites as a whole, responding to regional issues and rerouting traffic when necessary to maintain optimal performance and availability for our customers.

Mobile

Mobile

Yahoo has multiple security controls in place to ensure mobile devices, software, and applications are protected against threats.

Mobile security at Yahoo

Yahoo actively relies on security policies to establish an authorized method for controlling mobile computing devices including but not limited to:

- Flash Drives
- Handheld Wireless Devices
- Mobile Peripherals (e.g. USB port devices, CDs, mobile hotspots, etc.)

Security policies surrounding mobile devices apply to employees, consultants, vendors, and contractors.

Software development kits (SDKs)

Software development kits are a crucial component of Yahoo's mobile app development environment. SDKs allow engineers to integrate with new features and seamlessly access external services to create more dynamic application. However SDKs can also be susceptible to backdoor threats, potential improper data handling, and privacy violations. To mitigate potential threats, Yahoo has secure procedures in place for scenarios where third-party mobile SDKs are integrated with Yahoo products. Procedures include, but are not limited to:

Product Security Reviews

- SDK Integration Architecture Review
- SDK Scanning
- Penetration Testing

Mobile controls

The following are examples of controls implemented at Yahoo to mitigate and reduce unwanted behavior and potential exposure:

Mobile computing and storage devices containing or accessing information resources at Yahoo must have a valid business reason prior to connecting

Personal communication, mobile computing, and storage devices are prohibited from storing any cardholder information

Approved company portable computing devices and electronic storage media that contain confidential cardholder data to other sensitive information must use encryption or equally strong measures to protect the data while it is being stored.

Laptops, PDAs, smartphones, and other mobile devices must require a valid MDM profile, including username and password, which enforces Yahoo security policy.

Cloud security

Cloud security

Yahoo's cloud security controls are designed to protect the confidentiality and integrity of the data and applications that Yahoo stores on the public cloud.

Cloud security overview at Yahoo

The use of cloud computing technology and services continues to increase at a significant rate. Yahoo's strategy is no exception to this trend - Yahoo is continually putting more and more data onto the public cloud infrastructure due to cloud's superior performance and scalability. At Yahoo, securing the public cloud is paramount. The Cloud Security team at Yahoo describes a set of requirements and controls to uphold Yahoo's Information Security Policy regarding the protection of data and applications that are hosted on the public cloud infrastructure. Yahoo uses numerous cloud security controls designed to protect the confidentiality and integrity of its data and applications hosted on the public cloud. Yahoo's Cloud Security, Security Architecture, Vulnerability Management, and Risk/Compliance teams work together to develop and deploy a robust set of policies, standards, technologies, and controls to bolster and drive the security of Yahoo's public cloud. Yahoo has explicit security requirements ranging from identity and access management mechanisms to logging and monitoring systems to uphold Yahoo's public cloud infrastructure to appropriate security standards.

Identity and access management

Yahoo's identity and access management requirements abide by the principle of least privilege. Controls include a strong password and access key management policy, multifactor authentication requirements, and strict account provisioning and revocation requirements.

Logging and monitoring

A robust logging system is critical to providing a detective control for the public cloud infrastructure. Yahoo uses industry standard configurations to ensure that events in critical logs are properly alerting authorized Yahoo personnel. Unauthorized access and unexpected changes to resources is required to be monitored on all instances. This also serves as a check for incorrectly assigned permissions to users at Yahoo who may have received unintended access.

Networking

Yahoo account owners are required to establish secure network configurations. Some of the industry-standard configurations used include changing default resource settings (including the default access control list) and restricting inbound traffic to explicit destinations and protocols using carefully crafted ACLs on all Yahoo subnets.

Application protection

Yahoo implements several controls on the public cloud in order to protect its application stack. All connections are required to be encrypted to ensure that the data transmitted is protected. Using encrypted transmissions can ensure that the encrypted traffic between the edge servers and the custom origin cannot be unsealed by malicious users in case they are able to capture packets. The ciphers used for these transmissions are regularly reviewed to ensure they are not outdated.

Load balancers

Yahoo uses load balancing to ensure that fault tolerance is provided across applications. The load balancer serves as a single point of contact to ensure availability and prevent the disruption of service. Yahoo's account owners are required to follow a centralized cloud security standard to securely configure load balancers and ensure that they are protected from potential malicious activity.

Data protection

Yahoo has several standards and controls in place to protect the data transmitted and stored. Yahoo implements and maintains a robust key

management system to ensure that the lifecycle of all encryption keys is properly administered. All machine images are required to be encrypted and shielded from public access. They are required to be updated regularly in order to ensure they have the latest security updates. All data volumes and snapshots as well as those of other critical databases on the public cloud infrastructure are required to be encrypted and shielded from the public in order to secure the data stored inside of them.