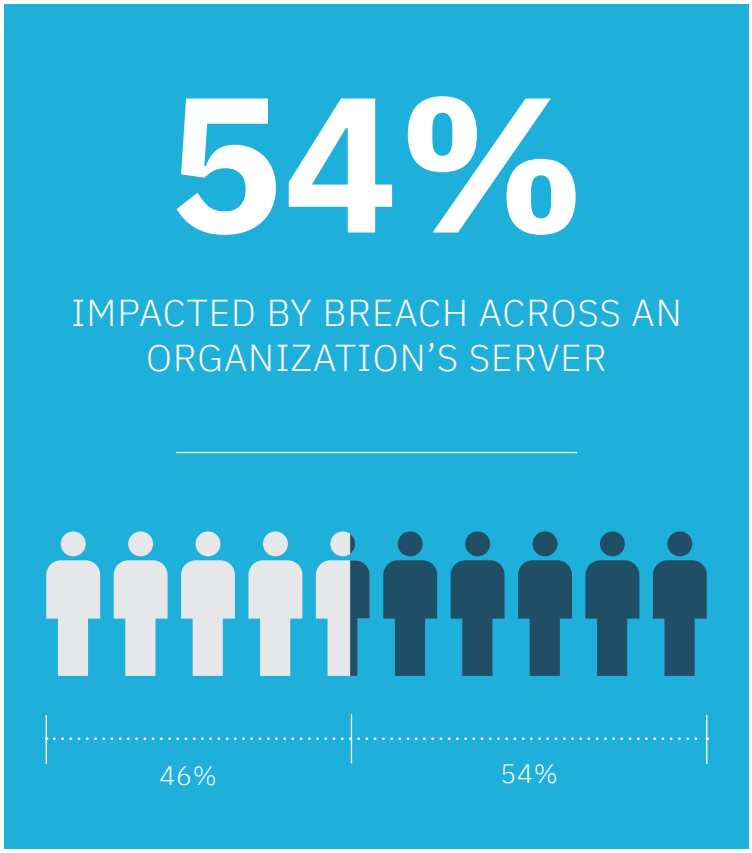
CLEARWATER
CYBERINTELLIGENCE INSTITUTE™

INSIGHT BULLETIN

Highest Level of Security Weaknesses in Hospitals and Health Systems Uncovered

More than half (54%) of all individuals affected by a healthcare information breach in the past twelve months were impacted by a breach that touched the affected organization's server, according to data provided on the U.S. Department of Health and Human Services Office for Civil Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. According to the data, ninety (90) healthcare breaches — affecting more than nine million individuals — were related to servers in some way.

Our studies show 62.83% of all critical and high risks are caused by some inadequately addressed security vulnerability in servers.



CAUSE FOR CONCERN

Servers are critical information system components, providing a central repository of data and critical programs that are shared by users across a hospital or health system network. Protecting the sensitive data that moves across these servers is essential to patient safety. Clearwater's CyberIntelligence® Institute (CCI) analyzed critical and high risks facing hospitals and health systems in our database over the past six months and confirmed, as suspected, that servers topped the list of information system components responsible for these risks, with 62.83% of all critical and high risks being caused by some inadequately addressed security vulnerability in these devices.

Top Server Vulnerabilities Creating the Highest Risks

DORMANT ACCOUNTS

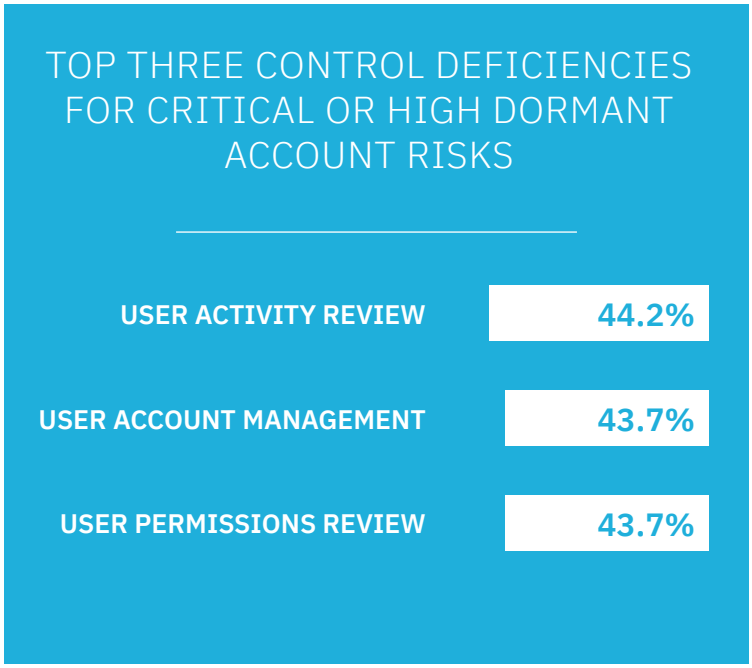
The Vulnerability

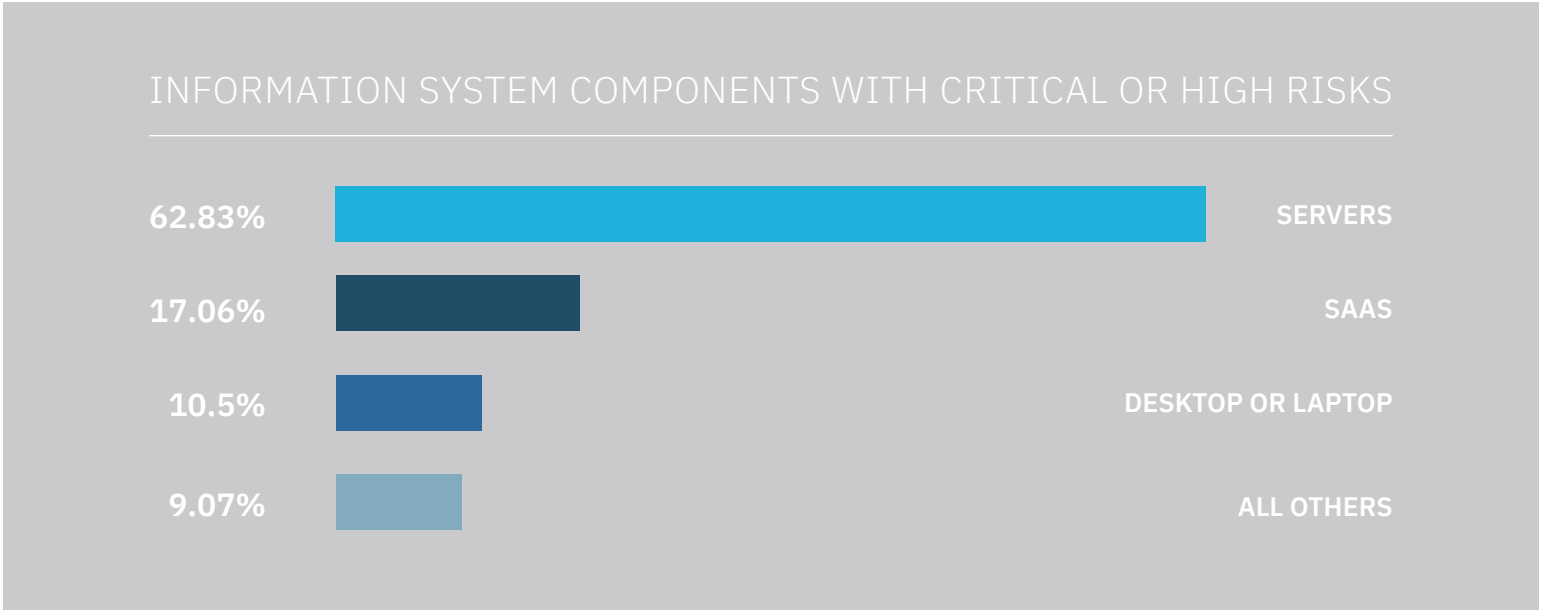
This vulnerability emerges when the accounts of users who no longer require access to an application, device, or system, usually due to their departure or a change of jobs, are not removed in a prompt manner (recommended 48 hours). This allows another user—usually a malicious internal party—to utilize the dormant account to access, change, or delete the information system's data in an unauthorized manner with little fear of detection, since they can employ a "valid" user account to mask their activities. The more dormant accounts an information system has and the longer these dormant accounts are present, the greater the likelihood that one or more of these accounts may be used in an illicit manner.

Prevention

Dormant account risks can be easily prevented through the use of security controls that automatically disable or remove an information system's user accounts when a change in employee status is entered into a human resources or payroll system. Where such system integration is not possible, frequent, periodic reviews of an information system's user permissions by appropriate system owners or managers can be used to identify user accounts that need to be disabled or removed. Likewise, frequent, periodic reviews of system activity logs, where these exist, by log analysis programs or by appropriate system owners or managers, can be used to spot the unauthorized use of dormant accounts and quickly remedy this problem.

Not surprisingly, therefore, information systems' dormant account risk was found to be highest when one or more of these important security controls was missing or inadequate, as the chart below shows:





EXCESSIVE USER PERMISSIONS

The Vulnerability

This security vulnerability results from giving information system users more access or more system rights (e.g. ability to add, edit, or delete records) than the job they perform requires. Not only is this an insecure practice, but it also violates the HIPAA Privacy Rule's principle of Least Privilege. Users with more system permissions than they require can inadvertently or intentionally access, change, or delete sensitive records (e.g. patient data) in an unauthorized manner.

Prevention

As with the dormant accounts vulnerability, some excessive user permissions created due to job changes can be prevented by disabling or changing information system access when a job change is recorded in a human resources or payroll system. Frequent, periodic reviews of user permissions by the appropriate system owner or manager can reveal users whose system permissions exceed what they require. Likewise, automated activity log reviews or frequent, periodic system activity reviews by the appropriate system owner or manager can disclose possible unauthorized activity by certain users and, if the information system logs the user activity, the information regarding the actual person who performed this unauthorized activity may be recorded.

Again, information systems' excessive user permissions risk was found to be highest when one or more of these important security controls was missing or inadequate, as the chart below shows:

TOP THREE CONTROL DEFICIENCIES FOR CRITICAL OR HIGH EXCESSIVE USER PERMISSION RISKS

USER PERMISSIONS REVIEW	43.6%
USER ACTIVITY REVIEW	43.6%
USER ACCOUNT MANAGEMENT	43.1%

Critical Steps to Secure Your Organization's Servers

Preventing an organization's server from falling prey to dormant account and excessive user permission vulnerabilities can be most readily accomplished by implementing the security controls that most effectively prevent or detect them. Here are some recommendations as to how to appropriately accomplish this for the three most relevant security controls:

01: USER ACTIVITY REVIEW

For larger information systems, manual review of user activity logs is simply impractical. Even for smaller systems, manual reviews of system activity logs can be very tedious. As a result, the use of "log analyzer" software that can automatically aggregate and analyze activity logs is recommended. However, while log analysis software can help to spot anomalies in user activity (e.g. large numbers of records viewed, changed, or deleted by a single user), such applications are most useful when they can correlate events occurring among multiple systems, a feature most often found in Security Incident and Event Management (SIEM) software. A program with this functionality can more likely readily identify potential malicious activity caused by multiple system weaknesses. For example, by correlating network logs with application logs, a security analysis program might show that an unusually high number of unauthorized record views were being conducted by a user that had successfully logged into the application remotely from China, which occurred one day after a large phishing email attack on the organization.

02: USER ACCOUNT MANAGEMENT

The user account management control entails automated coordination of user account access with systems that maintain user "position" (e.g. V.P, Manager, Line Employee, etc.) and "status" (e.g. employed, formerly employed, retired, etc.) information. Often, this coordination is achieved through the use of Identity Access Management systems that tie Active Directory access and group membership to human resource or payroll applications. However, organizations that have their own programming staff have also been known to write their own PowerShell scripts to achieve the same functionality many Identity Access Management programs provide. Nonetheless, if changes in employee positions and status are not recorded in a prompt manner, such programs will be ineffective in curbing dormant account and excessive user permission vulnerabilities. Identity Access Management programs also will not necessarily help curb these vulnerabilities in programs that manage user access and permissions internally and without reliance on Active Directory.

03: USER PERMISSIONS REVIEW

When organizations do not employ Identity Access Management programs like those mentioned previously, manual reviews of user system permissions are strongly recommended. The frequency of such reviews will be dictated by the number of system users and the frequency of user turnover. However, for those systems with 100 or more users, user permission reviews conducted at least quarterly are recommended. Where system access is also granted to students, a review of system permissions immediately after the end of a term or semester is also highly advisable.

About Clearwater CyberIntelligence® Institute

Clearwater delivers cyber risk management solutions to hundreds of healthcare delivery organizations and their partners. Clearwater's IRM|Analysis™ software facilitates and strengthens an organization's cyber risk management program by providing an automated, scalable process for assessing, remediating and monitoring the security risks to the organization's critical business systems and sensitive data while maintaining the evidence necessary for an audit or investigation.

The enormous data set of cyber risk information stored in our IRM|Analysis™ database enables us to capture deep insights surrounding current cyber threats and identify trends that will help inform and prepare organizations to Manage Cyber Risk Right. The Clearwater CyberIntelligence Institute, using its advanced analytics and data mining capabilities, has discovered significant patterns from our database which contains millions of data risk records from hospitals, Integrated Delivery Networks (IDNs) and business associates.

www.ClearwaterCompliance.com